SIEMENS

SINUMERIK

SINUMERIK 840Dsl/828D SINUMERIK Access MyMachine / OPC UA

Configuration Manual

Valid for:

OPC UA server Version 3.1

10/2020
6FC5397-1DP41-0BA5

Legal information

Warning notice system

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

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

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

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

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

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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

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

Trademarks

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

Disclaimer of Liability

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

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

Document order number: 6FC5397-1DP41-0BA5
Ⓟ 10/2020 Subject to change

Preface

SINUMERIK documentation

The SINUMERIK documentation is organized into the following categories:

- General documentation/catalogs
- User documentation
- Manufacturer/service documentation

Additional information

You can find information on the following topics at the following address (https://support.industry.siemens.com/cs/document/108464614/):

- Ordering documentation/overview of documentation
- Additional links to download documents
- Using documentation online (find and search in manuals/information)

If you have any questions regarding the technical documentation (e.g. suggestions, corrections), please send an e-mail to the following address (mailto:docu.motioncontrol@siemens.com).

mySupport/Documentation

At the following address (https://support.industry.siemens.com/My/ww/en/documentation), you can find information on how to create your own individual documentation based on Siemens' content, and adapt it for your own machine documentation.

Training

At the following address (http://www.siemens.com/sitrain), you can find information about SITRAIN (Siemens training on products, systems and solutions for automation and drives).

FAQs

You can find Frequently Asked Questions in the Service&Support pages under Product Support (https://support.industry.siemens.com/cs/de/en/ps/faq).

SINUMERIK

You can find information about SINUMERIK at the following address (http://www.siemens.com/sinumerik).

Target group

This document addresses commissioning engineers, machine tool manufacturers, planners and plant operating companies. The document provides detailed information that commissioning engineers require to setup the SINUMERIK Access MyMachine / OPC UA software.

Benefits

The Configuration Manual instructs the target group on how to use/configure the software correctly.

Standard scope

This documentation describes the functionality of the standard scope. Additions or revisions made by the machine manufacturer are documented by the machine manufacturer.

Other functions not described in this documentation might be executable in the control system. This does not, however, represent an obligation to supply such functions with a new control system or when servicing.

For the sake of simplicity, this documentation does not contain all detailed information about all types of the product and cannot cover every conceivable case of installation, operation, or maintenance.

Note regarding the General Data Protection Regulation

Siemens observes standard data protection principles, in particular the principle of privacy by design. That means that this product does not process / store any personal data, only technical functional data (e.g. time stamps). If a user links this data with other data (e.g. a shift schedule) or stores personal data on the same storage medium (e.g. hard drive) and thus establishes a link to a person or persons, then the user is responsible for ensuring compliance with the relevant data protection regulations.

Technical Support

Country-specific telephone numbers for technical support are provided in the Internet at the following address (https://support.industry.siemens.com/cs/sc/2090/) in the "Contact" area.

If you have any technical questions, use the online form in the "Support Request" area.

Table of contents

Introduction 1

1.1 General description

Uniform standard for data exchange

"Industrie 4.0" stands for the intensive utilization, evaluation and analysis of data from the production in IT systems of the enterprise level. PLC programs today already record a wide range of data at the production and process level (pressure values, temperatures and counter readings) and make them available to systems at the enterprise level, for example, to increase the product quality. With Industry 4.0, the data exchange between the production and enterprise levels will increase much faster in the future. However, prerequisite for the success of "Industrie 4.0" is a uniform standard for data exchange.

The **OPC UA (Unified Architecture)** standard is particularly suitable for data exchange across different levels as it is independent from specific operating systems, has secure transfer procedures and better semantic description of the data. OPC UA not only makes data available, but also provides information about the data (e.g. data types). This enables machine-interpretable access to the data.

1.1.1 SINUMERIK OPC UA server

The SINUMERIK OPC UA server offers a communication interface with manufacturer independent standard. The information on SINUMERIK controls can be exchanged with an OPC UA client using this communication interface.

The client is not part of SINUMERIK and is either part of standard software or can be developed as part of individual software. For this purpose a stack for downloading is provided by the OPC foundation.

Some manufacturers provide a software development kit, which can be used to develop an OPC UA client.

1.2 Features

The SINUMERIK OPC UA server provides the possibility to communicate with SINUMERIK via OPC UA. The following functionalities of the OPC UA specification are supported by the server:

- Read, write and subscribe to SINUMERIK variables (NC, PLC) (see chapter Variable access (Page 94))
- Transfer of part programs (see chapter File system (Page 117))
- Support for File and Folder Objects
- Event based provision of SINUMERIK alarms and messages from HMI, NC and PLC (see chapter Alarms (Page 104))
- Methods for selection of part programs from the NC file system and external memory (see chapter Select (Page 126)) and methods for tool management (see chapter Tool management (Page 130))
- Multi language support for the alarm and warning messages.
- The OPC UA server supports customer specific object models (see chapter Customer Specific Object Model (CSOM) (Page 41))

Security settings

The server provides the possibility to communicate in an unencrypted or encrypted way. The following options are possible:

- None
- 128 Bit - Sign (Basic128Rsa15)
- 128 Bit - Sign & Encrypt (Basic128Rsa15)
- 256 Bit – Sign (Basic256Sha256)
- 256 Bit - Sign (Basic256)
- 256 Bit – Sign & Encrypt (Basic256Sha256)
- 256 Bit - Sign & Encrypt (Basic256)

NOTICE
Security risk of no or low encryption During operational process, an encrypted communication must always be used for security reasons.

Furthermore, the SINUMERIK OPC UA server provides the possibility of user administration, which allows to assign access rights for each user individually (see chapter User administration (Page 83)).

See also

Certificate handling (Page 28)

1.3 System setup

Accessibility of the server

The accessibility of the server varies in the particular SINUMERIK systems. The following table shows the dependencies of the SINUMERIK systems:

SINUMERIK systems	Accessibility	
SINUMERIK 828D	After successful licensing and activation the OPC UA server is accessible via the X130 interface.	
SINUMERIK 840D sl	The OPC UA server needs SINUMERIK Operate and runs on the same place as SINUMERIK Operate. For this reason, system setup depends on whether a Thin Client is used (SINUMERIK Operate runs on NCU) or a PCU / IPC with Windows operating system.	
	Thin Client	If a Thin Client is used, the OPC UA server is accessible after successful licensing and activation via X120 and X130 interface of the NCU.
	PCU / IPC	If a PCU / IPC is used, the OPC UA server is accessible after successful licensing and activation via "eth1" and "eth2" interface of the PCU / IPC. In this case the OPC UA server is neither accessible via "eth3" interface of the PCU/IPC nor the X120 or X130 interface of the NCU.

Application scenario

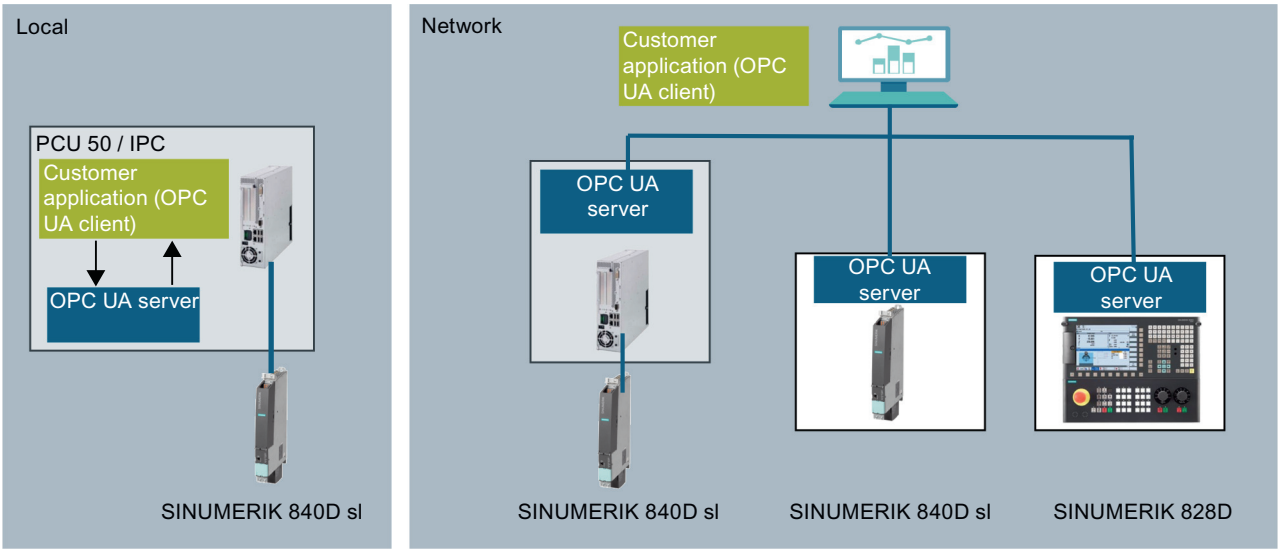


Figure 1-1 Application scenario

1.4 Compatibility of OPC UA server version and CNC software versions

The latest OPC UA server version is compatible to several CNC software versions.

CNC software versions:

- 4.5
- 4.07 - SP2...SP5
- 4.08 - SP2...SP3
- 4.92 and 4.92 - HF2
- 4.93
- 4.94

1.5 Reference to OPC UA specification

The SINUMERIK OPC UA server matches the specification of the OPC foundation (https://opcfoundation.org/) V1.0.3.

Safety notes 2

2.1 Fundamental safety instructions

2.1.1 General safety instructions

⚠ WARNING

Danger to life if the safety instructions and residual risks are not observed

If the safety instructions and residual risks in the associated hardware documentation are not observed, accidents involving severe injuries or death can occur.

- Observe the safety instructions given in the hardware documentation.
- Consider the residual risks for the risk evaluation.

⚠ WARNING

Malfunctions of the machine as a result of incorrect or changed parameter settings

As a result of incorrect or changed parameterization, machines can malfunction, which in turn can lead to injuries or death.

- Protect the parameterization against unauthorized access.
- Handle possible malfunctions by taking suitable measures, e.g. emergency stop or emergency off.

2.1.2 Warranty and liability for application examples

Application examples are not binding and do not claim to be complete regarding configuration, equipment or any eventuality which may arise. Application examples do not represent specific customer solutions, but are only intended to provide support for typical tasks.

As the user you yourself are responsible for ensuring that the products described are operated correctly. Application examples do not relieve you of your responsibility for safe handling when using, installing, operating and maintaining the equipment.

2.1.3 Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit
https://www.siemens.com/industrialsecurity (https://www.siemens.com/industrialsecurity).

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under
https://www.siemens.com/industrialsecurity (https://new.siemens.com/global/en/products/services/cert.html#Subscriptions).

Further information is provided on the Internet:

Industrial Security Configuration Manual (https://support.industry.siemens.com/cs/ww/en/view/108862708)

⚠ WARNING

Unsafe operating states resulting from software manipulation

Software manipulations, e.g. viruses, Trojans, or worms, can cause unsafe operating states in your system that may lead to death, serious injury, and property damage.

- Keep the software up to date.
- Incorporate the automation and drive components into a holistic, state-of-the-art industrial security concept for the installation or machine.
- Make sure that you include all installed products into the holistic industrial security concept.
- Protect files stored on exchangeable storage media from malicious software by with suitable protection measures, e.g. virus scanners.
- On completion of commissioning, check all security-related settings.

2.2 OPC UA security notes

NOTICE
OPC UA provides read/write access on data in SINUMERIK. This access might also affect security relevant data. • You can limit this access on SINUMERIK data by individual read and write permission or by using an own object model and deactivating the SINUMERIK namespace. Please refer to chapter User administration (Page 83), especially chapter "List of access rights".

Note

Communication and system performance

Please note that the OPC UA server is not a real-time enabled process that, depending on client requirements, generates a corresponding communication load in the SINUMERIK system. Increased communication load can have repercussions on system performance.

The SINUMERIK system load may vary with different part programs.

A high system load can have repercussions on communication performance.

See also

List of access rights (Page 86)

Setting up of OPC UA server

3

3.1 Prerequisites

NOTICE
Protection against security risks To protect industrial plants and systems comprehensively against cyber attacks, measures must be applied simultaneously at all levels (from the operational level up to the field level, from access control to copy protection). Therefore, before setting up of the OPC UA server, apply the "Defense in Depth" protection concept in order to avoid security risks in your environment. Ensure that you do not connect the company network to the internet without suitable protective measures. You will find **further information** on the Defense-in-Depth concept, suitable protective measures and Industrial Security in general in the Configuration Manual Industrial Security (https://support.industry.siemens.com/cs/de/en/view/108862708).

Prerequisites

- OPC UA server requires SINUMERIK Operate.
- OPC UA server requires an OPC UA license (6FC5800-0AP67-0YB0 (paper license), 6FC5800-0AP67-0YH0 (electronic license)).
- Make sure that the HMI time is set correctly, since this is a prerequisite for encrypted communication.

3.2 Option OPC UA

Setting the option

1. Set the "Access MyMachine / OPC UA" option via the "Startup > Licenses" operating area.

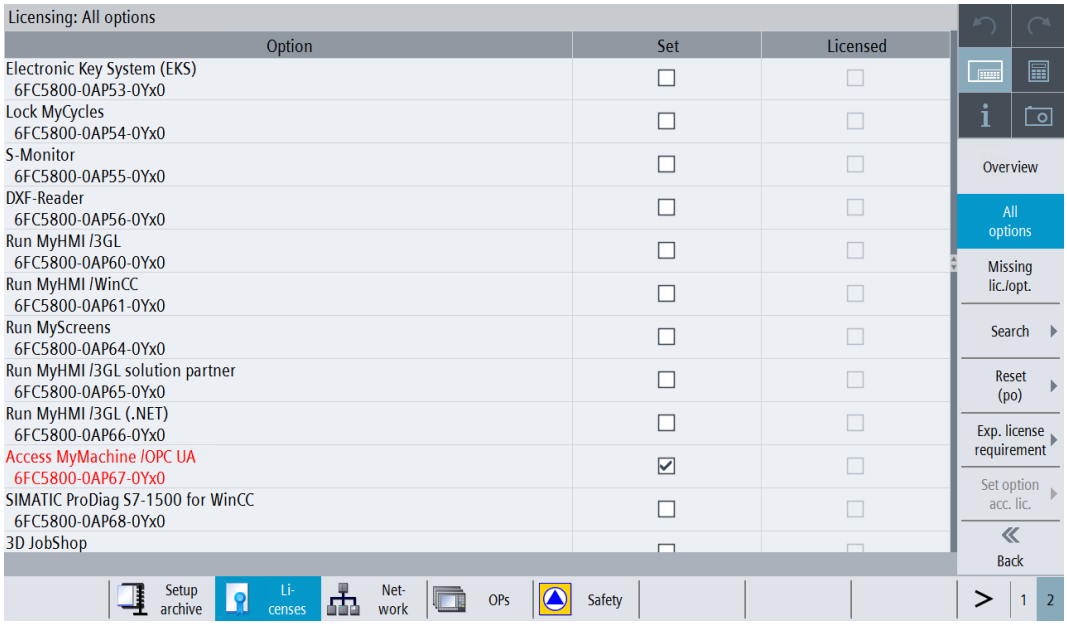


Figure 3-1 Setting the option

3.3 Commissioning

Checking the HMI time

Make sure that the HMI time is set correctly, since this is a prerequisite for encrypted communication.

Note

The certificate needed for secure OPC UA communication is automatically created during the first run-up. The start date of the validity period of the certificate is set to the current date. The validity period is 20 years.

If the SINUMERIK system time is subsequently changed, so that it lies outside the validity period, the secure OPC UA communication does not function (BadCertificateTimeInvalid).

The certificate can also be changed manually, as described in chapter Certificate handling (Page 28).

Executing the OPC UA configuration dialog

1. Start the OPC UA configuration dialog via the operating area "Startup > Network".

   Note

   Different startup behavior with 828D / V4.5

   The control 828D with CNC software version V4.5 has a different startup behavior of the configuration dialog (see chapter Starting of configuration dialog (Page 166)).

2. Press the "OPC UA" softkey.

3. Press the "Setting" softkey. The Settings dialog will appear. Then press the "Change" softkey. Make the necessary settings for connection and activation.

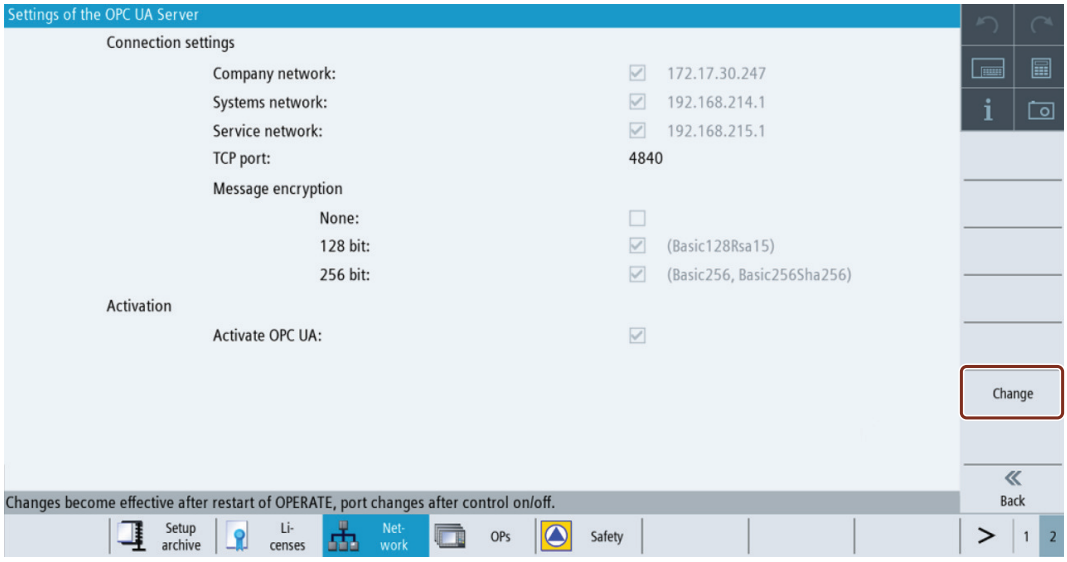


Figure 3-2 Settings of OPC UA Server (with changes)

<table>
<tr><th>Group</th><th>Setting</th><th>Description</th></tr>
<tr><td rowspan="4">Connection settings</td><td rowspan="2">• Company network
• Systems network (machine network)
• Service network</td><td>The available network connections (IP address) on a specific target system (828D, 840D sl, PCU, IPC) are shown. The available networks options vary depending on your target system.
• Company network
• Systems network (machine network)
• Service network.
For example, since IPC is considered as PCU there will be only two networks (company and systems (machine) network) displayed.
OPC UA clients running on the same IPC as the OPC UA server can reach the server through the company or system network IP addresses. The OPC UA server cannot be reached through local host address (127.0.0.1).
It is possible to activate or deactivate an interface from OPC UA server point of view.</td></tr>
<tr><td>TCP Port</td><td>TCP port at which the OPC UA server should be available.
Standard configuration: 4840
Note!
The port must also be open in the firewall. For PPU/NCU this happens automatically. With PCU/IPC the port must be opened manually in the firewall.</td></tr>
<tr><td>Message encryption</td><td>It can be chosen which security endpoints should be offered from the server
Note!
By default strongest message encryption cannot be disabled.
<table><tr><th>Setting</th><th>Standard configuration</th></tr><tr><td>None</td><td>Deactivated</td></tr><tr><td>128 bit</td><td>Activated</td></tr><tr><td>256 bit</td><td>Activated</td></tr></table></td></tr>
<tr><td>Activation</td><td>Activate OPC UA</td><td>Place the checkmark to activate OPC UA and remove the checkmark to deactivate it.</td></tr>
</table>

NOTICE

Security risk due to data manipulation and data sniffing

Anonymous access can be a security risk. Anonymous access should therefore be strictly limited to commissioning.

- For normal operation authentication via username and password or based on certificates should be used (see chapter Certificate handling).

NOTICE
Security risk due to data manipulation and data sniffing If no message encryption to the client is established, there will be a security risk of data manipulation and data sniffing. It is therefore highly recommended to establish a message encryption to the client. • Use the highest possible encryption standard (256 bit) to ensure a secure message transfer.

Note

DNS based addressing

If you want to contact the OPC UA server via host name you have to do the following steps:

- Set the host name in SINUMERIK Operate. You can find further information on setting the host name in SINUMERIK Operate in the Commissioning manual "Basesoftware and operating software" (https://support.industry.siemens.com/cs/ww/en/view/109777907).
- Afterwards go to the certificate dialogue of the OPC UA server and renew the server certificate with "DNS only" (see chapter Server certificates (Page 29)).

Now the OPC UA server can be addressed via host name.

Please consider that for

- NCU
  - System network is DHCP/DNS server
  - Company network is DHCP/DNS client
- IPC
  - System and company network is DHCP/DNS client
  - Company network is DHCP/DNS client

For addressing the OPC UA server via company network you must ensure that the central DNS server uses the same host name as given in Operate.

4. Then press "OK". If you enter a port for the first time, you will receive a safety note.

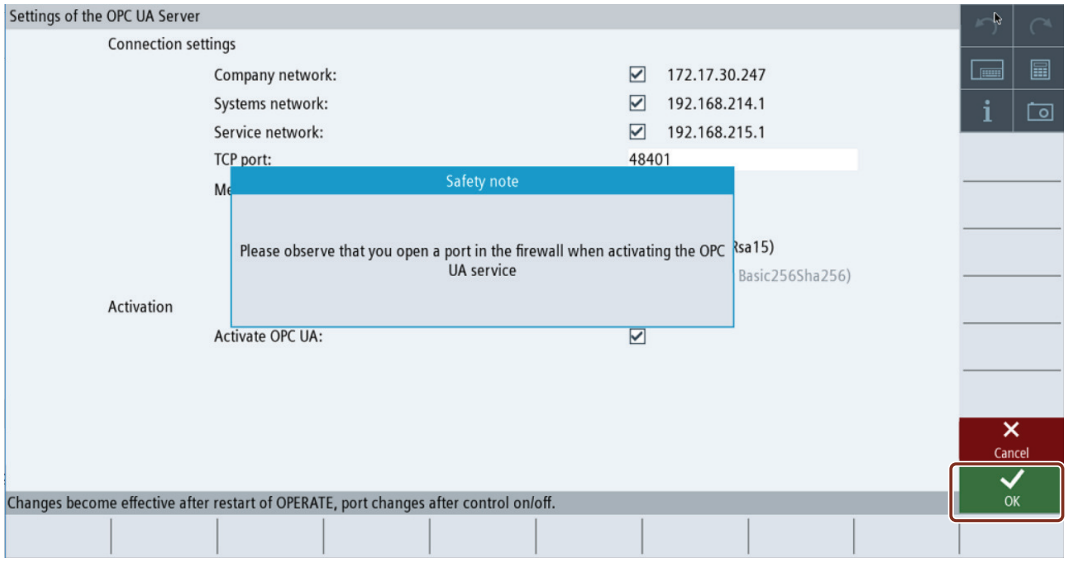


Figure 3-3 Safety note opening TCP port

Note

Port opening on IPC

On first startup of OPC UA server a windows message will appear, asking the user to confirm the opening of the port.

5. To confirm the opening of the port, press "OK".
6. To perform the authentication settings, press "Back", and then press the "Authentication" softkey. The Authentication dialog will appear.

7. Press the "Change" softkey. Make the necessary settings for authentication.

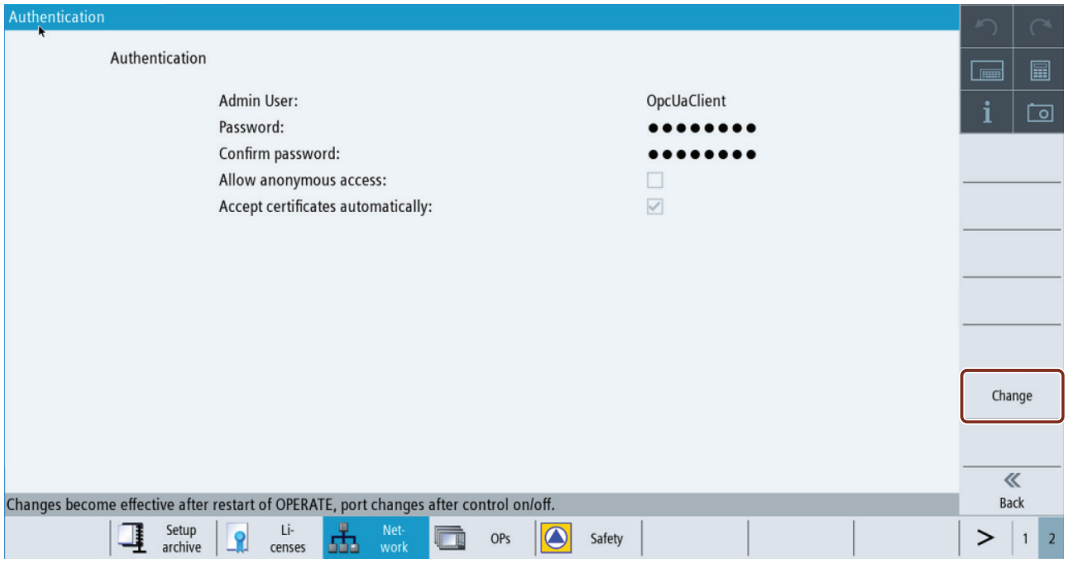


Figure 3-4 Authentication settings of OPC UA server

Group	Setting	Description
Authentication	Admin User	User name of the administrator. The administrator can add or delete users and assign or delete user authorizations.
	Password	Password of the administrator.
	Confirm Password	Enter the password again for confirmation.
	Allow anonymous access	Standard configuration: Deactivated Anonymous access is only recommended for commissioning.
	Accept certificates automatically	Standard configuration: Activated If this option is set, all client certificates are automatically accepted. For manual acceptance, please refer to chapter Certificate handling (Page 28).

Note

Assigning secure passwords

Observe the following rules when creating new passwords:

- When assigning new passwords, ensure that you do not assign passwords that can be guessed, e.g. simple words, key combinations that can be easily guessed, etc.
- Passwords must always contain a combination of upper-case and lower-case letters as well as numbers and special characters. Passwords must comprise at least eight characters. The server does not support passwords comprising less than eight characters. PINS must comprise an arbitrary sequence of digits.
- Wherever possible and where it is supported by the IT systems, a password must always have a character sequence as complex as possible.

The German Federal Office for IT Security (BSI) (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/International/GSK_15_EL_EN_Draft.pdf?__blob=publicationFile&v=2) provides additional rules for creating secure passwords.

Programs are available that can help you to manage your passwords. Using these programs, you can encrypt, save and manage your passwords and secret numbers – and also create secure passwords.

Note

If you want to change the password later, you can do this via the OPC UA method "ChangeMyPassword" or in the SINUMERIK Operate screen.

8. If settings are all done, restart is necessary to activate the new settings. Perform a hardware restart on the target systems NCU and PPU. A restart of SINUMERIK Operate is necessary on the PCU 50/IPC.

3.4 Certificate handling

3.4.1 Overview

To establish a secure connection between an OPC UA server and a client it is necessary to exchange and trust the certificate of the other communication partner. The exchange is normally done automatically at the first connection attempt between client and server. Nevertheless, there is also the possibility to exchange the certificates manually before the other communication partner is available, e. g for preparing an easy commissioning.

For trusting the certificates there are two possibilities within the server:

- Automatic trusting of new certificates
  If "Accept certificates automatically" is activated in the commissioning dialog, new client certificates are trusted automatically and there is no manual interaction necessary to establish a secure connection.
  This is the most comfortable option, but less secure than the manual trusting, since all certificates will be trusted.
- Manual trusting of certificates (recommended)
  If "Accept certificates automatically" is deactivated in the commissioning dialog the certificates must be trusted manually to establish a secure connection.
  This allows the administrator of the OPC UA server to manually decide, which client can establish a secure connection to the OPC UA server

To have a comfortable way to handle certificates, the OPC UA dialog offers a certificate section, which can be found under the softkey "Certificates".

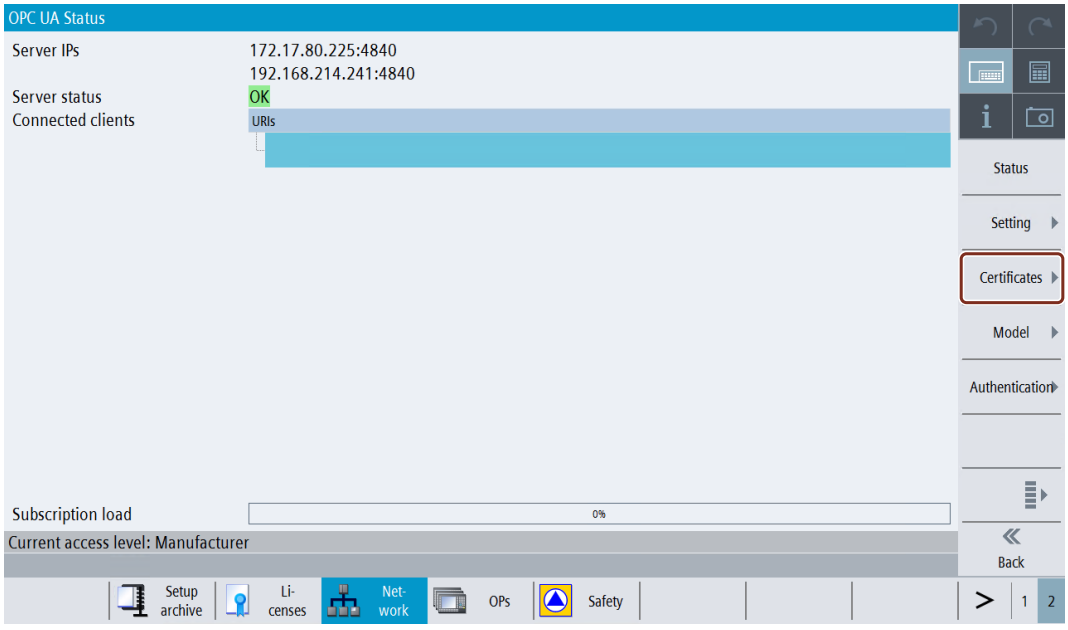


Figure 3-5 Softkey Certificates

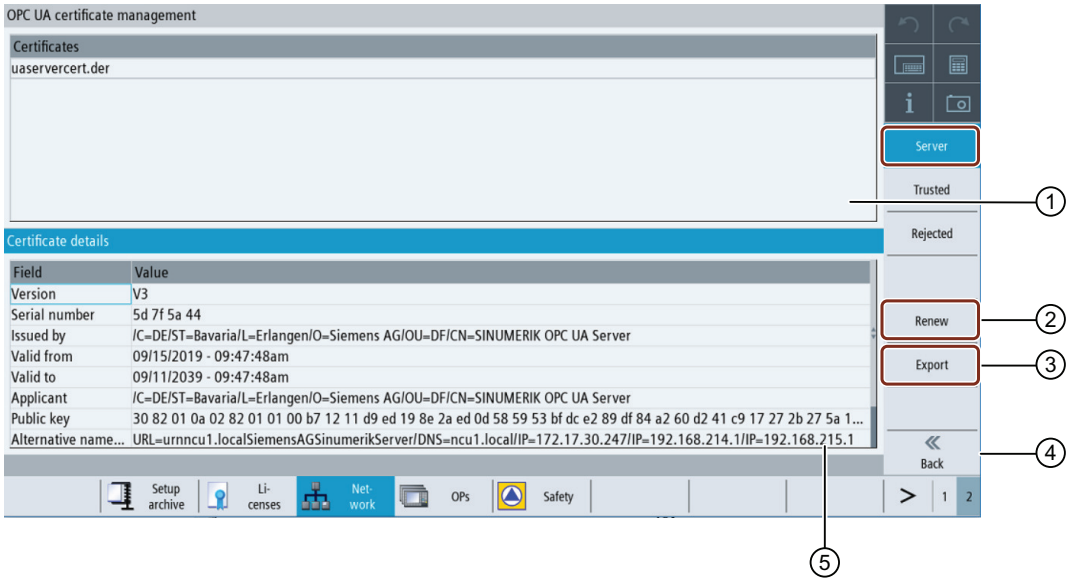
Operations

The Certificate dialog allows the following operations:

- Server certificate
  - Renewal of the server certificate
  - Export of the current server certificate
- Client certificates
  - List of the current trusted certificates
  - List of the rejected client certificates
  - Manual import of a client certificate
  - Deletion of a client certificate
  - Trust a rejected client certificate

3.4.2 Server certificates

Overview



① The name of the OPC UA server certificate is shown in the upper part of the screen.
② You can renew the server certificates.
③ You can export the server certificate to a configured device.
④ You can leave the OPC UA dialogs.
⑤ The details of the server certificate are shown in the lower part of the screen. You can scroll down to see further certificate attributes.

Figure 3-6 Server Certificate

Renewing server certificates

The server certification can be renewed at any time. With the renewal the following things can be specified by the administrator:

- Expiration date of the certificate / validity in years

  Note

  Before using this dialog make sure that the date and the time of SINUMERIK Operate is set correctly, as the certificate will be valid from the current date in SINUMERIK Operate at the time of renewal.

- Decision if IP address and/or DNS name should be mentioned in the server certificate

  Note

  Many clients will need the IP address in the certificate for validation. If the server will be addressed by DNS name (e. g. because the IP address of the OPC UA server changes frequently due to a dynamic assignment by a DHCP server), it is recommended only to include the DNS name in the certificate. Because otherwise the certificate must be renewed and exchanged with every change of the IP address.

To renew a server certificate, proceed as follows:

1. Press the softkey "Renew".
   A pop-up screen will appear that offers two ways of selecting a time period:
   - Select the number of years, the server certificate will be valid
   - Specify a precise date, the server certificate will expire

   Specify also whether the IP address and/or the DNS name should be written in the server certificate.

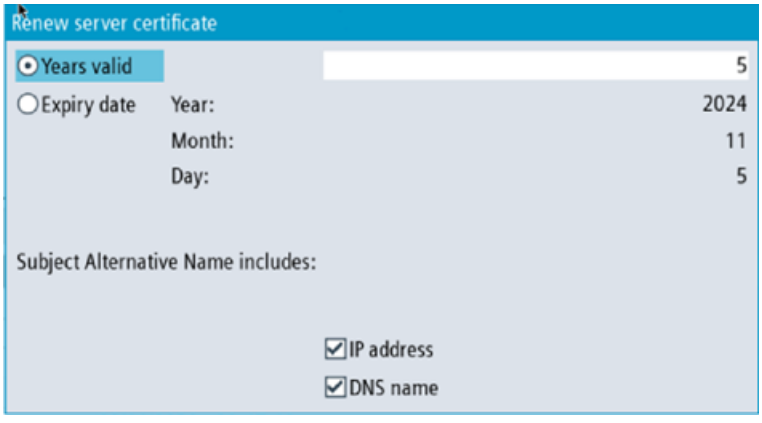


Figure 3-7 Renew server certificate

Pressing the softkey "Cancel" will ignore all input and return to the "Server" dialog.
Pressing the softkey "Ok" will save the input to the system, the currently valid certificate will be deleted and with the next start of SINUMERIK Operate the new certificate gets created.

Exporting server certificates

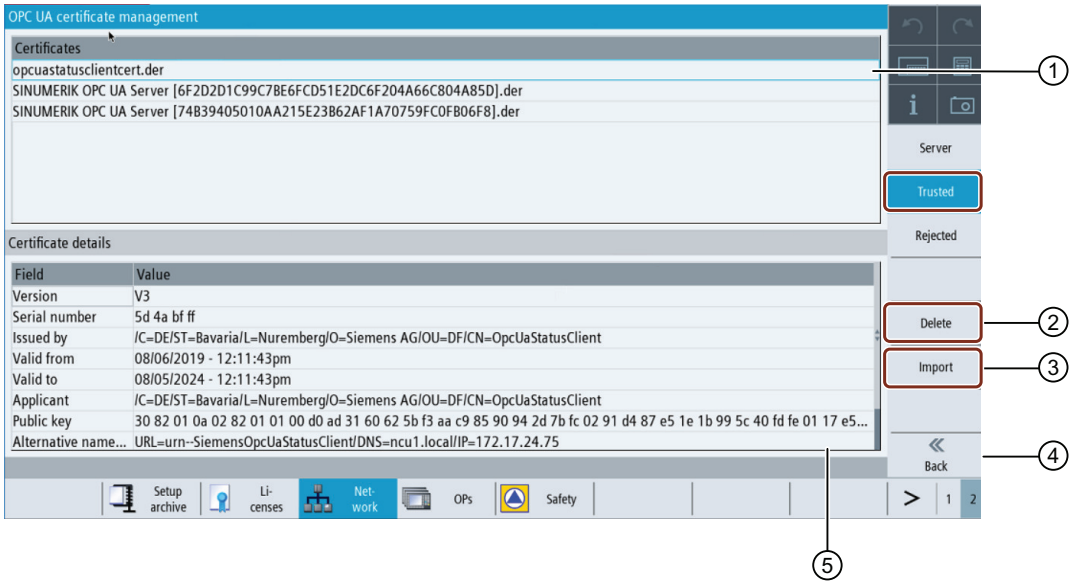
For an offline preparation of the connection to the server, you can export the server certificate. After that the certificate can be imported and trusted on the client side.

1. Press the softkey "Export".
   A pop-up screen will appear showing the USB device to export to. You can navigate to a location on the USB device to export the OPC UA server certificate.
   Pressing the softkey "Cancel" will ignore all input and return to the "Server" dialog.
   Pressing the softkey "Ok" will export the certificate.

3.4.3 Client certificates

3.4.3.1 Trusted certificates

Overview



① The trusted certificates are listed in the upper part of the screen. You can select a certificate using the arrow keys (cursor up/ cursor down).

② You can delete the trusted certificates.

③ You can import a certificate from an USB device.

④ You can leave the OPC UA dialogs.

⑤ The certificate details are shown in the lower part of the screen. To set the focus on the lower part of the screen the softkey "next window" on the keyboard is used.

Figure 3-8 Trusted Certificate

Deleting trusted certificates

1. To manually delete a client certificate select a certificate in the trusted list and press the softkey "Delete".
   A pop-up screen will appear asking you for confirmation of deletion:

Figure 3-9 Delete certificate

Pressing the softkey "Cancel" will do no action and return to "Trusted" dialog.
Pressing the softkey "Ok" will delete the selected certificate.

Note

After the deletion of the client certificate a connection with OPC UA server can no longer be established by the client of the corresponding certificate.

Importing certificates

To prepare a connection a client certificate can be imported before actually establishing a connection. With the import the certificate is automatically trusted.

1. Press the softkey "Import".
   A pop-up screen will appear showing the USB device to import from. You can navigate to a location on the USB device to import a certificate to a trusted folder.
   Pressing the softkey "Cancel" will ignore all input and return to the "Trusted" dialog.
   Pressing the softkey "Ok" will import the certificate.

Note

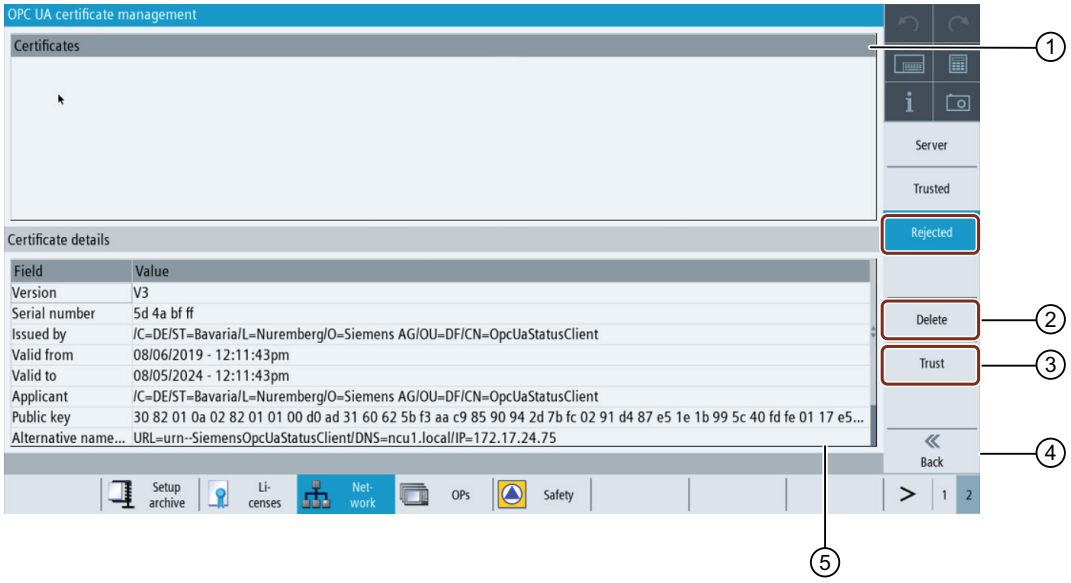
Keep in mind, that only certificates with the file extension "*.der" are accepted.

Note

To use a certificate for authentication it is necessary to create a user with the method "AddCertificateUser" first.

3.4.3.2 Rejected certificates

Overview



① The rejected certificates are listed in the upper part of the screen. You can select a certificate using the arrow keys (cursor up/ cursor down).

② You can delete the selected certificate.

③ You can trust the selected certificate.

④ You can leave the OPC UA dialogs.

⑤ The certificate details are shown in the lower part of the screen. To set the focus on the lower part of the screen the softkey "next window" on the keyboard is used.

Figure 3-10 Rejected Certificate

Deleting rejected certificates

1. To manually delete a client certificate, select the certificate in the rejected list and press the softkey "Delete".
   A pop-up screen will appear asking you for confirmation of deletion:

Figure 3-11 Delete rejected certficate

Pressing the softkey "Cancel" will do no action and return to the previous dialog.
Pressing the softkey "Ok" will delete the selected certificate.

Trusting rejected certificates

If the setting "Accept certificates automatically" is deactivated, certificates automatically transferred by a client with the first connection attempt will be treated as untrusted and need to be trusted manually before the connection can be established. In this case, the server will report an error (BadSecurityChecksFailed) on initial connection attempt.

1. To manually trust a client certificate, select the certificate in the rejected list and press the softkey "Trust".
   A pop-up screen will appear asking for confirmation of trusting the certificate.

Figure 3-12 Trust certificate

   Pressing the softkey "Cancel" will return to the "Rejected" dialog.
   Pressing the softkey "Ok" will trust the certificate and move it to the trusted folder.

3.5 Testing the connection

Requirement

To test the connection, you can use the "Sample Applications" of the OPC Foundation (https://opcfoundation.org/developer-tools/specifications-unified-architecture/opc-unified-architecture-for-cnc-systems/) under "Developer Tools/Developer Kits/Unified Architecture". It is necessary to register with the OPC Foundation for this.

Note

There are two ways to establish the connection:

- Connection without security
- Connection with the security policy "Basic128Rsa15" respectively "Basic256" and the security mode "SignAndEncrypt"

SIEMENS always recommends setting up a connection with security, as only in this way the confidentiality of the data transmitted can be ensured.

Installation

The "Sample Applications" additionally install a service with the name "OPC UA Local Discovery Server". If you want to locally test the OPC UA connection, i.e. an installation directly on the PCU 50/IPC, you must deactivate this service.

Note

If the service "OPC UA Local Discovery Server" is active, the OPC UA server cannot be started correctly, because it blocks the needed TCP port 4840.

This service has no influence if the "Sample Applications" are installed on a PC in the network. Deactivation is then not necessary.

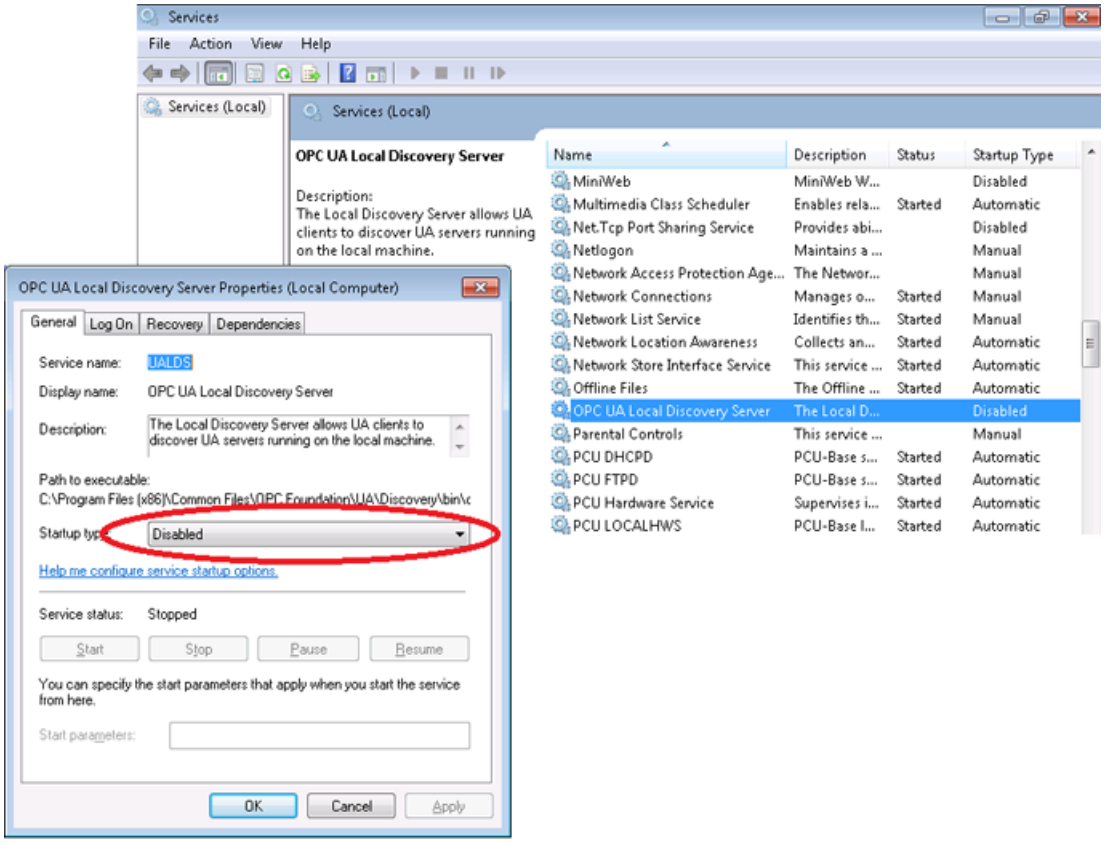


Figure 3-13 Deactivating the "OPC UA Local Discovery Server" service on PCU 50/IPC

Procedure

1. Start the OPC UA "Sample client".

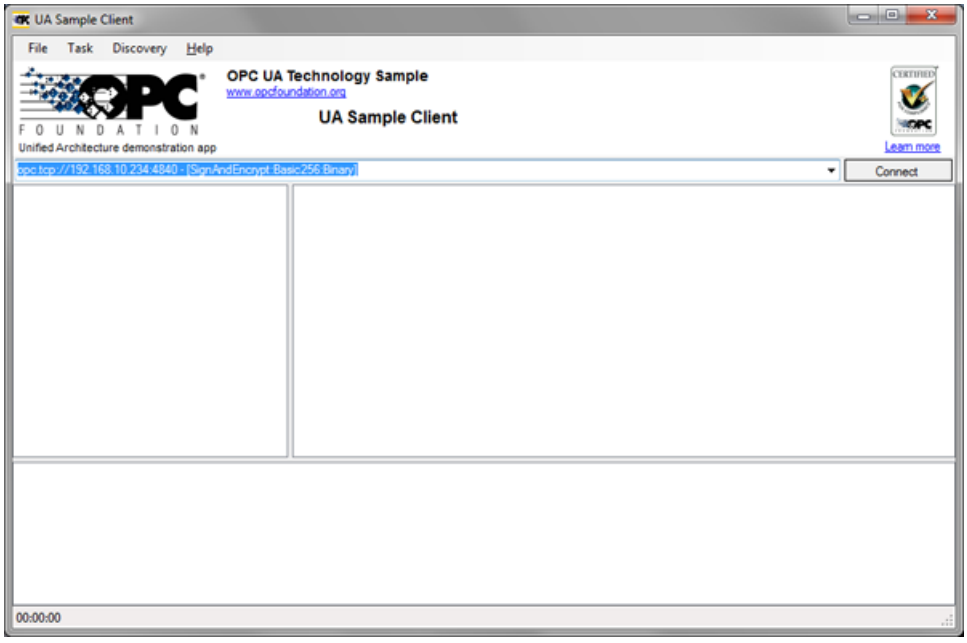


Figure 3-14 Sample Client main window

2. Select the "New" entry from the drop-down list.
   The "Discover Servers" window opens.
3. Now enter the IPv4 address of the target system and click the "Discover" button.

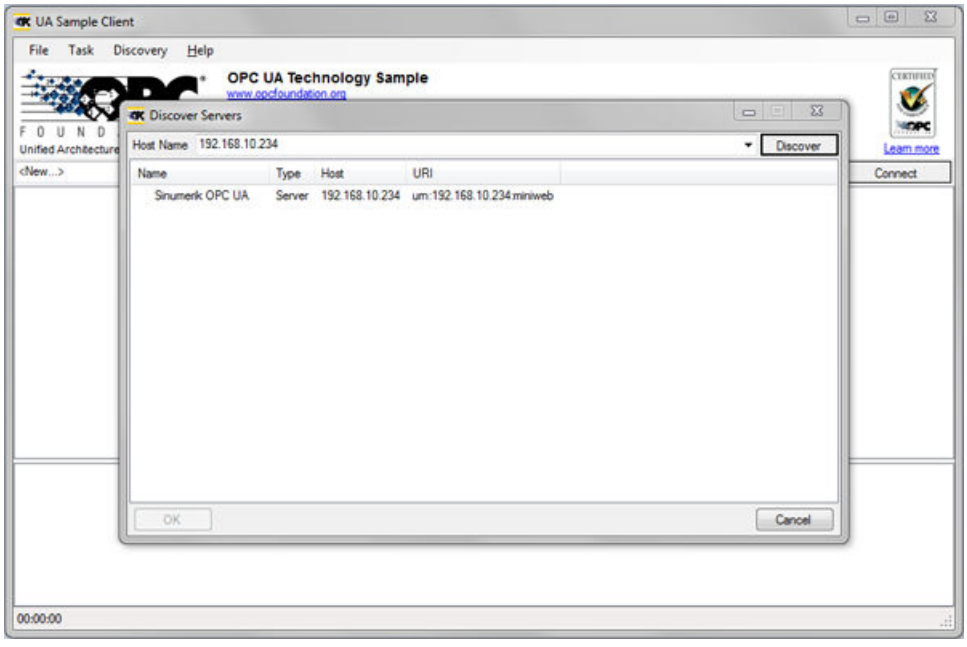


Figure 3-15 Discover servers

4. The SINUMERIK OPC UA server appears in the list. Select the server and confirm with "OK".
5. Return to the main window and click the "Connect" button.

6. To establish a simple connection without security, configure the following settings. After clicking "OK", enter the administrator user assigned when OPC UA was set up and the administrator password. Confirm your settings by clicking "OK".

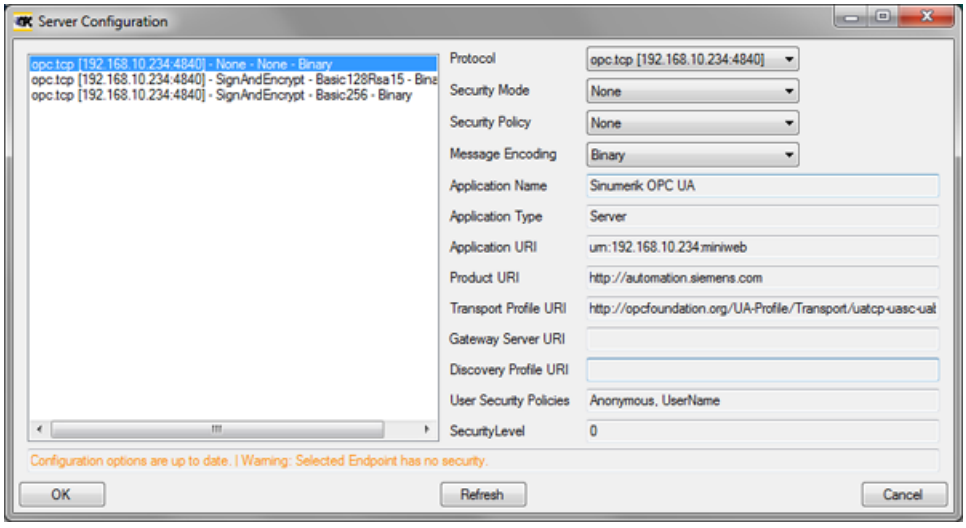


Figure 3-16 Server configuration

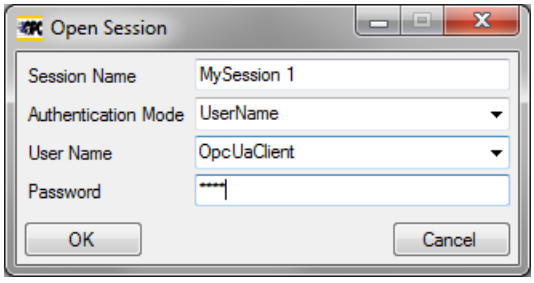


Figure 3-17 User Identity

7. Confirm the prompt asking if you want to trust the transferred certificate with "Yes".

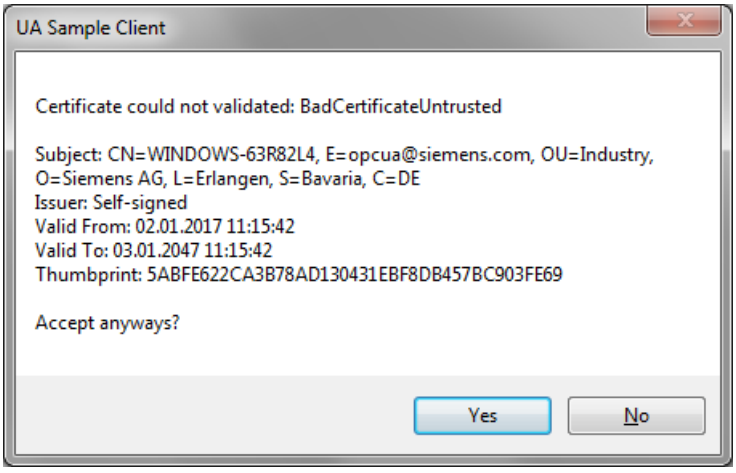


Figure 3-18 Certificate

The connection to the SINUMERIK OPC UA server is now established and the available address space is displayed.

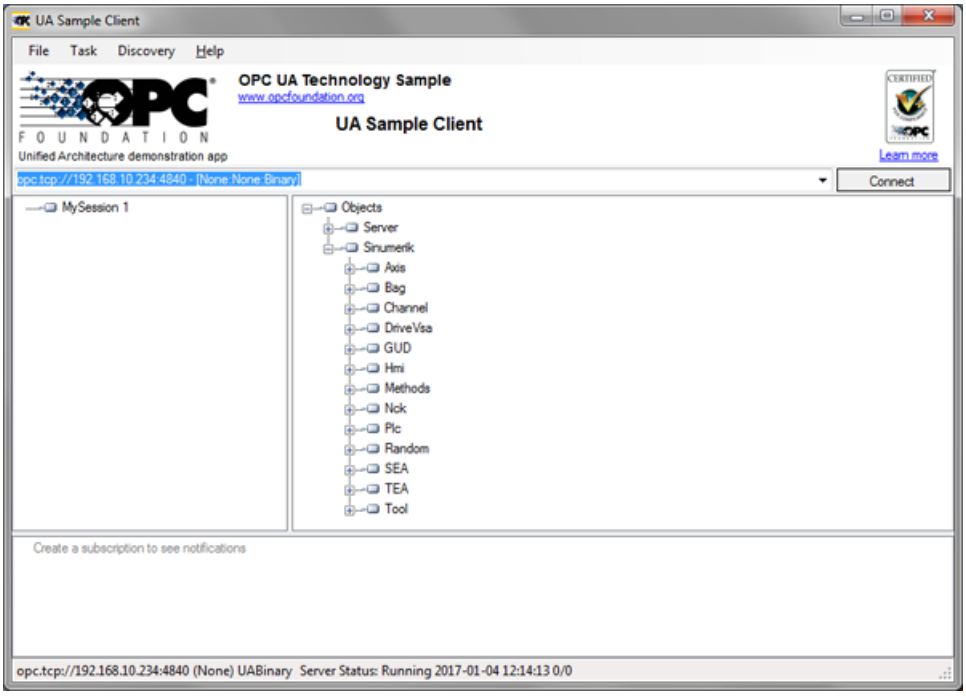


Figure 3-19 Address space of the SINUMERIK OPC UA server

8. Now navigate to a nodeID (e.g. R-parameter at Sinumerik > Channel > Parameter > R) and right click the corresponding entry. You can now test various functions:

– E.g. read, write, setup monitoring

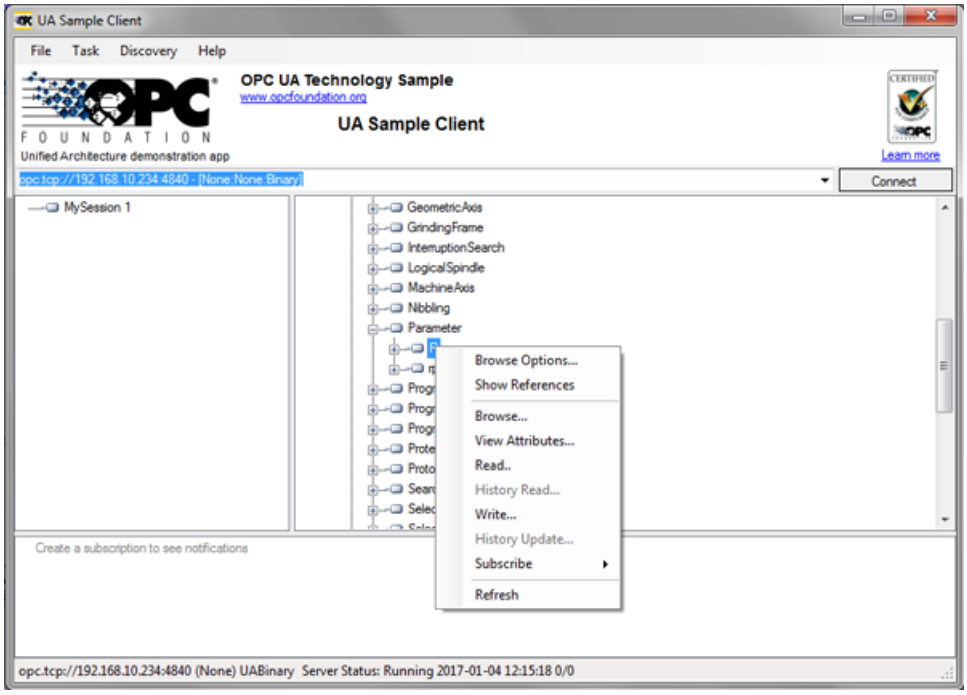


Figure 3-20 NodeID "Sinumerik > Channel > Parameter > R"

– The attributes of a NodeID can be queried via the entry "View Attributes". One of these attributes is the "Value", which provides the corresponding value of R1.

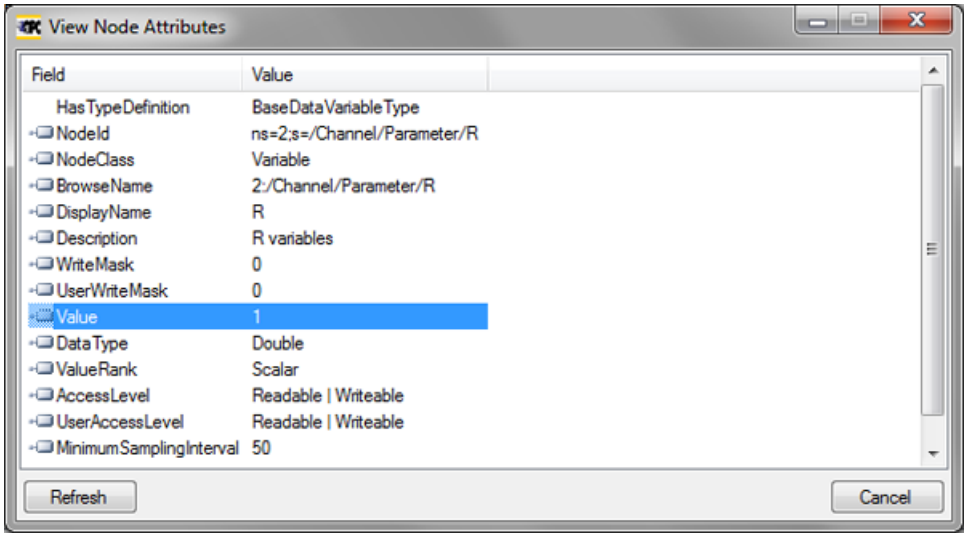


Figure 3-21 Viewing node attributes

Customer Specific Object Model (CSOM) 4

4.1 Overview

What is a Customer Specific Object Model (CSOM)?

The primary objective of the OPC UA address space is to provide a standard way for servers to represent objects to clients. The OPC UA object model has been designed to meet this objective. It defines objects in terms of variables and methods. It also allows relationships to other objects to be expressed.

A **C**ustomer **S**pecific **O**bject **M**odel allows a specific view of the OPC UA server to meet the requirements in a customer-specific project. For this purpose, you can specify all required OPC UA nodes in an XML file.

You can use several tools to create your own Object Model. In this manual, all processes and examples are explained on the base of the tool **SiOME** (**S**iemens **O**PC UA **M**odeling **E**ditor).

SiOME

With the help of SiOME, a tool for implementing Customer Specific Object Models or OPC UA companion specifications, you can:

- design information models / address spaces for your OPC UA server
- create new types and instances of OPC UA nodes
- map OPC UA variables to SINUMERIK variables
- enable multiple license in a single custom model (Page 63)

Download link and explanations about SIOME are available here (https://support.industry.siemens.com/cs/de/en/view/109755133).

4.2 Functionalities

What is possible with a CSOM?

Possible application scenarios for a CSOM could be the following:

- Implementation of an own Information model
- Modifying of an own information model:
  - structure
  - display name
  - browse name
  - description

What is not possible?

- Change of data types

Quantity structure of CSOM

Feature	Value
Maximum number of binary files	1
Maximum number of CSOM namespaces	7[1]
Maximum number of nodes in CSOM	10.000

(1) Maximum number of CSOM namespaces can be created is 6, if lisence namesapce is created. For more information, refer topic Modeling rules (Page 71).

4.3 Workflow for using CSOM in the SINUMERIK OPC UA server

4.3.1 Overview

In order to use a Customer Specific Object Model (CSOM), it is necessary to follow a certain workflow procedure.

The following chapter provides an overview about the necessary process steps. Every process step will also be covered in greater detail.

CSOM process workflow

The CSOM workflow consists of the following steps:

1. Exporting SINUMERIK model from OPC UA server as OPC UA XML with SINUMERIK Access MyMachine /P2P.
2. Creating a CSOM with SiOME (Page 45).
3. Converting the CSOM from XML to binary (Page 73) with SINUMERIK Access MyMachine / P2P.
4. Importing the CSOM into the SINUMERIK OPC UA server (Page 74) with SINUMERIK Operate.

See also

Exporting SINUMERIK model from OPC UA server as OPC UA XML (Page 43)

4.3.2 Exporting SINUMERIK model from OPC UA server as OPC UA XML

SiOME offers the possibility to map variables using drag and drop. In order to provide this usability, SiOME needs to know the SINUMERIK address space of the machine, where the CSOM should be implemented.

Since the address space depends on machine configuration, this address space has to be exported after commissioning of the machine using "SINUMERIK Access MyMachine /P2P".

SINUMERIK Access MyMachine /P2P is reading SINUMERIK address space via OPC UA browse functionality and providing an XML file to be imported into SiOME.

Prerequisites

For exporting SINUMERIK OPC UA model, it is necessary to have SinuReadAll access right.

SINUMERIK Access MyMachine /P2P

SINUMERIK Integrate Access MyMachine /P2P (MLFB 6FC5860-7YC00-0YA0) supports the commissioning of machines with SINUMERIK Operate (software version 2.6 and higher) using a standard Windows PC. Its scope of functions includes the exchange of files between the service PC and the control as well as operation of the HMI user interface. EasyScreen texts, alarm texts, tool management texts and other texts can be edited easily.

Exporting SINUMERIK OPC UA model as OPC UA XML

The following graphic shows the process of exporting the target system address space as OPC UA XML.

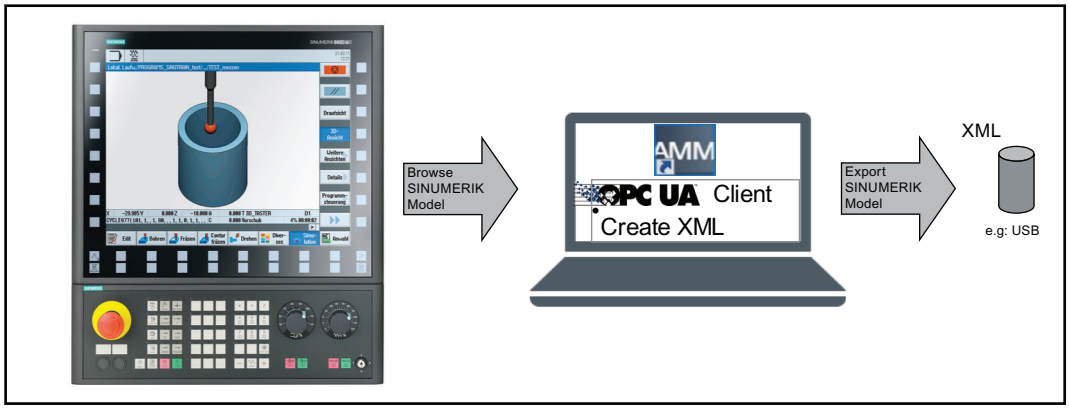


Figure 4-1 **Exporting SINUMERIK OPC UA model as OPC UA XML**

Procedure

1. Open the application "SINUMERIK Access MyMachine /P2P".
2. Click on "Tools > Sinumerik Opcua Server Tools > Opcua Server Model Export". A popup window appears.

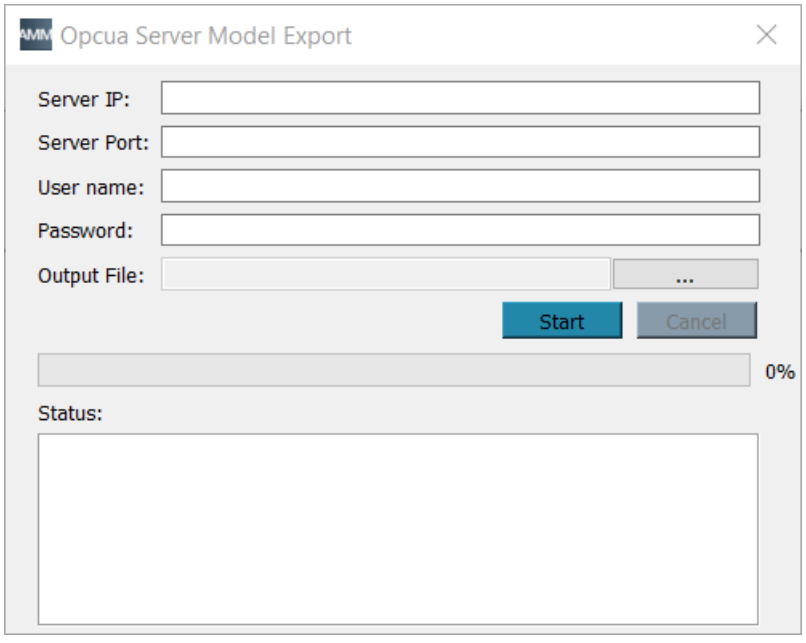


Figure 4-2 Opcua Server Model Export

3. Enter the IP address and the port of the OPC UA server as well as the username and password to access the server. Then specify where the output file should be saved to.
4. Click "Start" button to generate the xml file. The generated XML file is saved to the specified location.

The generated XML file can then be imported into SiOME tool.

4.3.3 Creating a CSOM with SiOME

4.3.3.1 Overview

SiOME is a free of charge tool from SIEMENS that allows to easily create an OPC UA object model and map the object either to SINUMERIK or SIMATIC S7-1500 variables.

The following chapter shows the engineering workflow for a CSOM with SINUMERIK and SiOME.

This process itself has 3 sub steps:

1. Importing SINUMERIK model (XML) (Page 45)
2. Modeling own object model (Page 48)
3. Exporting CSOM (XML) (Page 68)

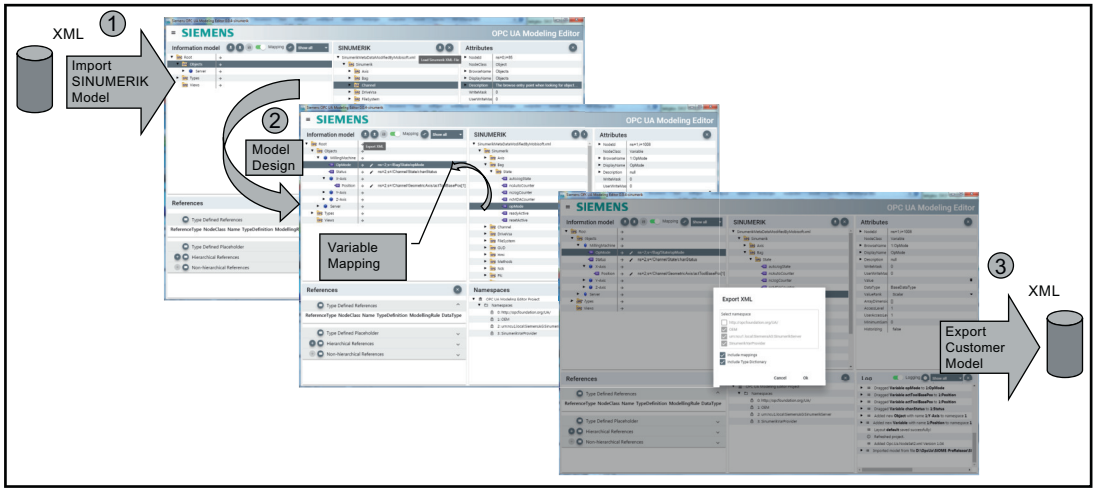


Figure 4-3 Creating a CSOM with SiOME

These 3 sub steps are explained further in the below sections with one application example.

4.3.3.2 Importing SINUMERIK model (XML)

Prerequisite

Exported SINUMERIK model (XML) file from SINUMERIK Access MyMachine /P2P.

Procedure

1. Open the SiOME application.
2. Click "Layout" drop down and select "SINUMERIK" as shown in the below image. The SINUMERIK layout is displayed.

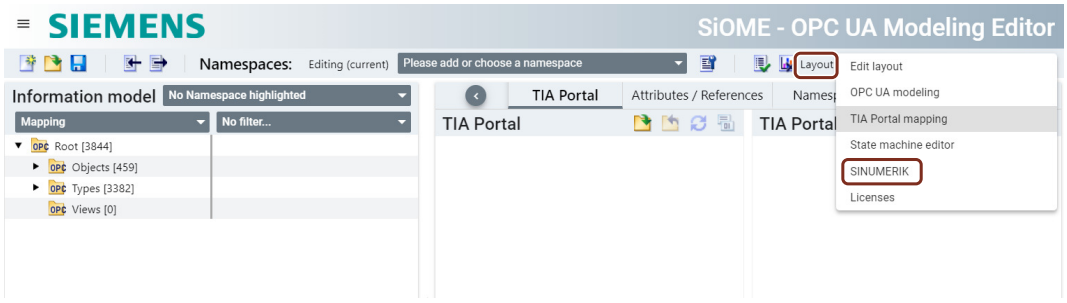


Figure 4-4 SiOME layout option

3. Click the icon in "SINUMERIK" tab to import the SINUMERIK model (XML) as shown in the below image.

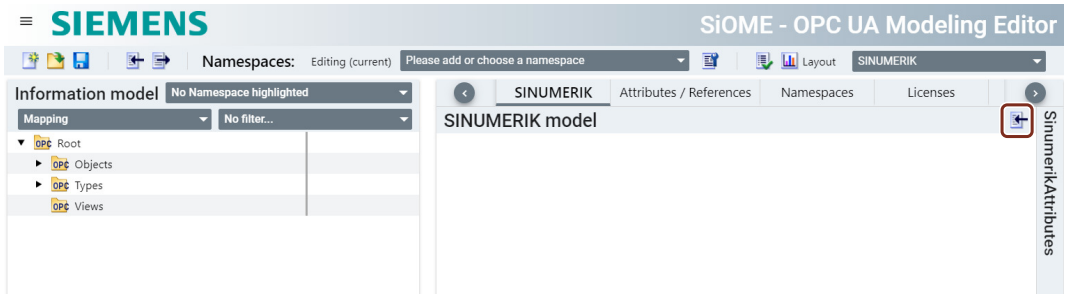


Figure 4-5 SiOME dashboard page

4. A "Open" dialog box appears. Select the exported SINUMERIK model (XML) file and then click "Open".

Result

SINUMERIK tab shows the SINUMERIK browse tree as shown in the below image:

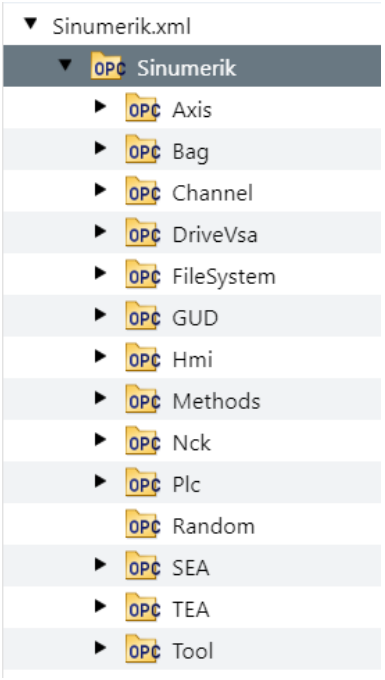


Figure 4-6 SINUMERIK tab with SINUMERIK browse tree

4.3.3.3 Modeling own object model

Creating new namespace

To create a new namespace, follow the below steps:

1. Click on "Please add or choose a namespace" and then click "Add New Namespace" as shown in the below image.
2. The "Add Namespace" popup window appears. Enter a name in the "Namespace URI" field and then click "Ok".

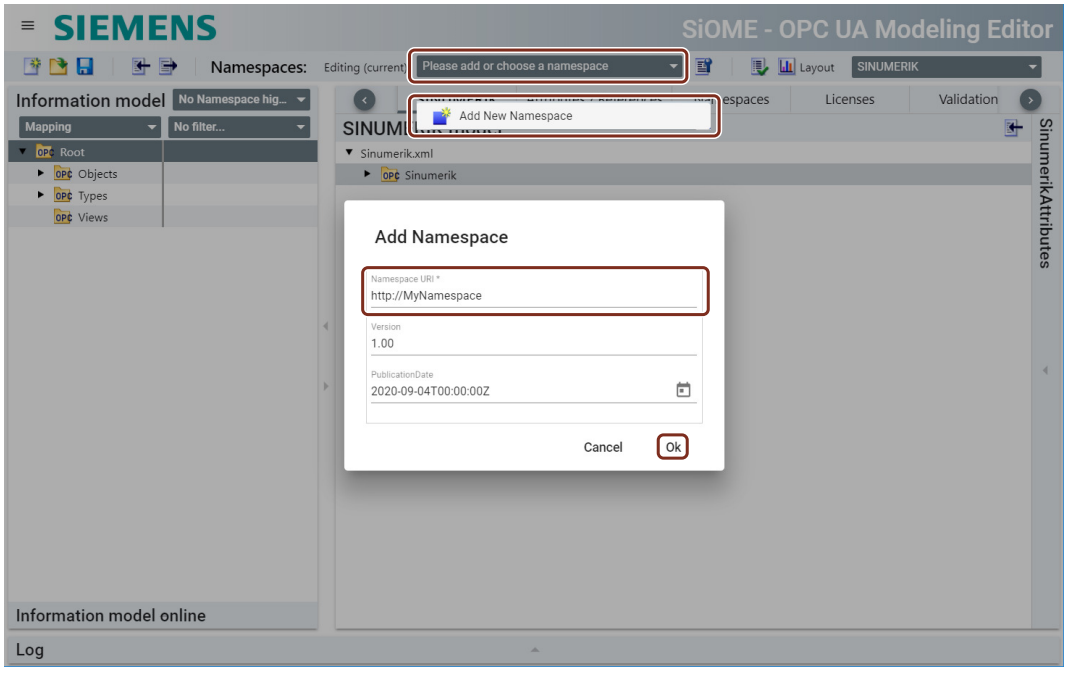


Figure 4-7 Adding new Namespace

Result

The new namespace is added in "Namespaces" tab.

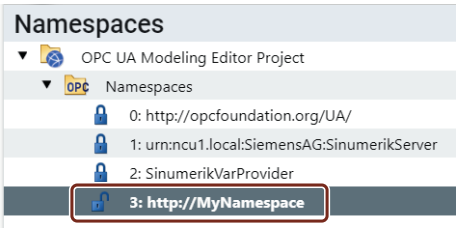


Figure 4-8 Namespace added

Creating a new object

To create a new object, follow the below steps:

1. Right-click on "Objects" node in "Information model" tab and then click on "Add Instance".

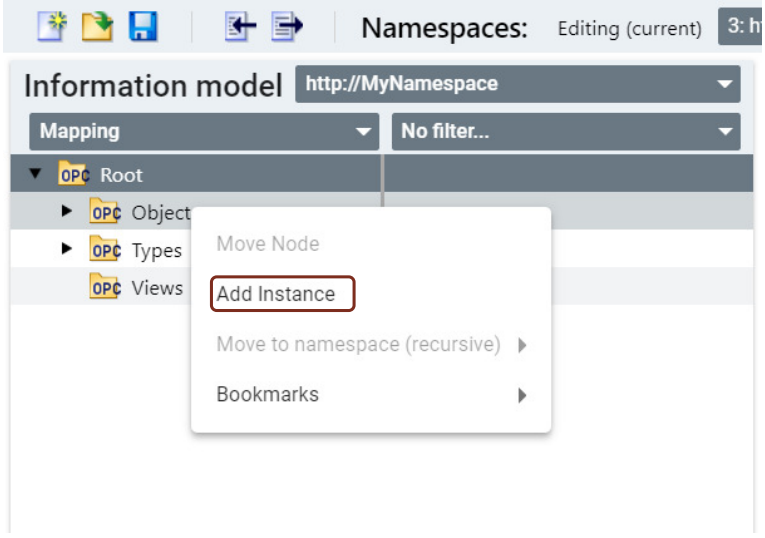


Figure 4-9 Information model tab

2. The "Add Instance" popup window appears. Enter a name in the "Name" field.

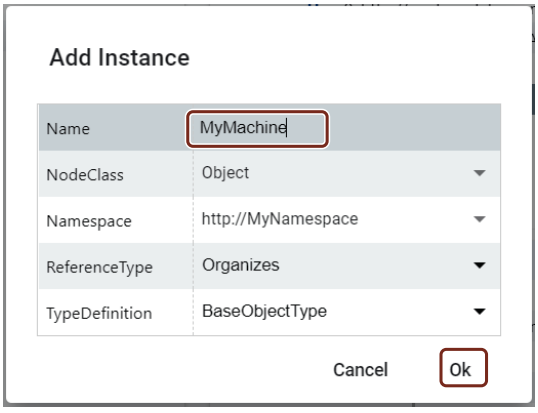


Figure 4-10 Add Instance popup window

3. Verify that newly added namespace is selected in the "Namespace" row and then click "Ok".

Result

The new instance is added under "Objects" node.

Adding a new instance for a variable

To add a new instance for a variable, follow the below steps:

1. Under "Objects" node, right-click on "MyMachine" node and then click on "Add Instance".

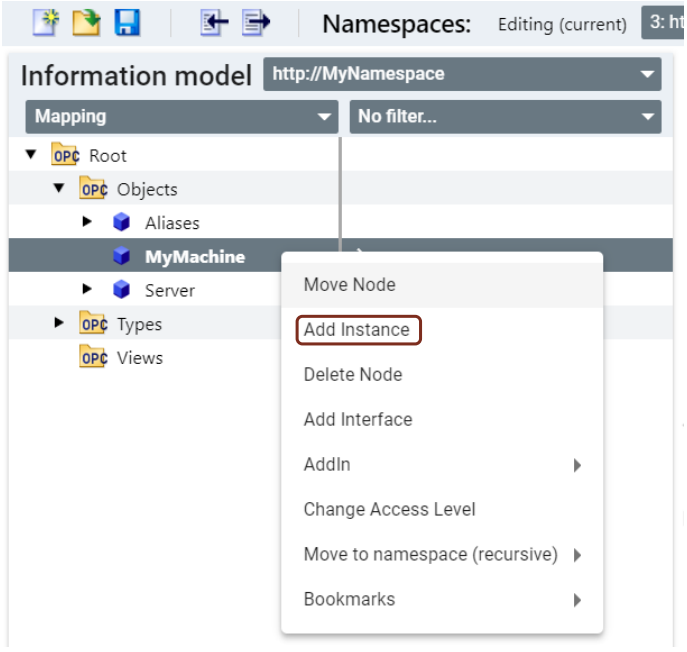


Figure 4-11 Adding a new instance for a variable

2. The "Add Instance" popup window appears. Enter a name in the "Name" field.
3. Select "Variable" from the "NodeClass" drop-down list.
4. Select "Double" from the "DataType" drop-down list and then click "Ok".

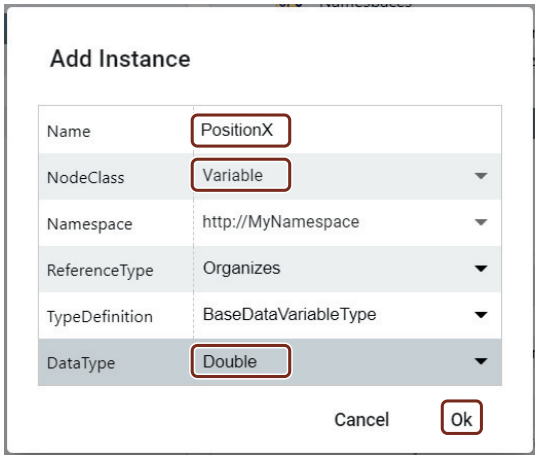


Figure 4-12 Add Instance popup for a variable

Result

The new instance is added for a variable under "MyMachine" node.

Mapping to SINUMERIK data

To map the SINUMERIK data, follow the below steps:

1. Drag and drop the variable from the "SINUMERIK" tab to the variable "PositionX" in the "Information model" tab as shown in the below image.

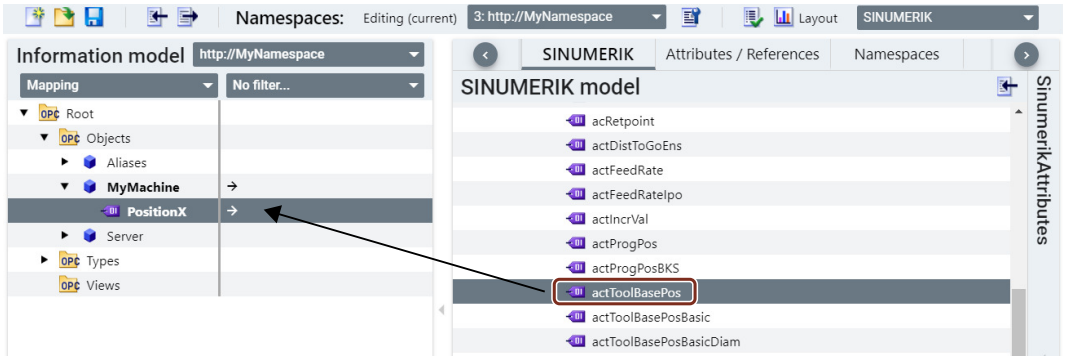


Figure 4-13 Mapping SINUMERIK variable

The variable is mapped in the mapping table in the "Information model" tab.

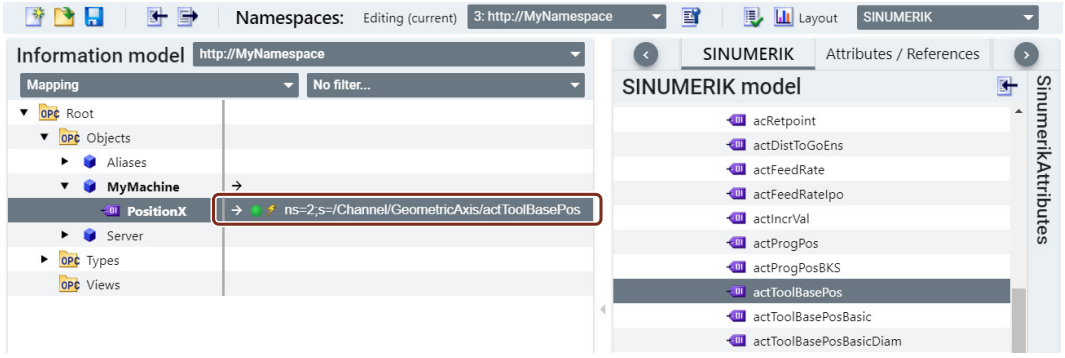


Figure 4-14 SINUMERIK variable mapped in mapping table

2. Add the correct axis index.

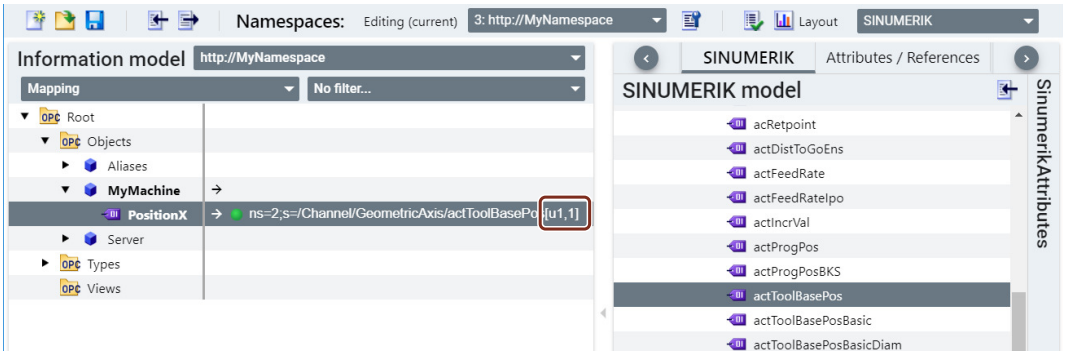


Figure 4-15 Adding axis index

Note

Do not edit the namespace value (for instance, ns=2). If edited, it will not be considered.

Adding a method node in CSOM

Method nodes can be added in two ways:

- Direct drag and drop under custom object.
- Adding a new instance variable and mapping the method from SINUMERIK tab.

Direct drag and drop under custom object

To add a method, press and hold the **ctrl** button and drag and drop the method from the "SINUMERIK" tab to the "MyMachine" node as shown in the below image.

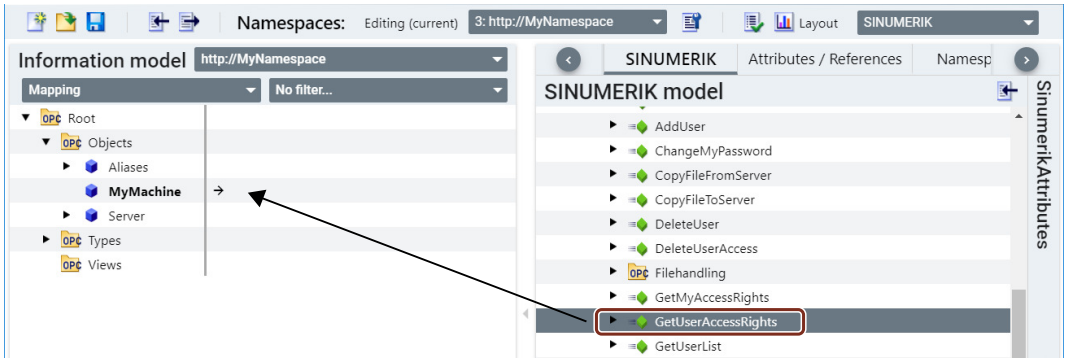


Figure 4-16 Mapping SINUMERIK method

The method is added under "MyMachine" node in the "Information model" tab.

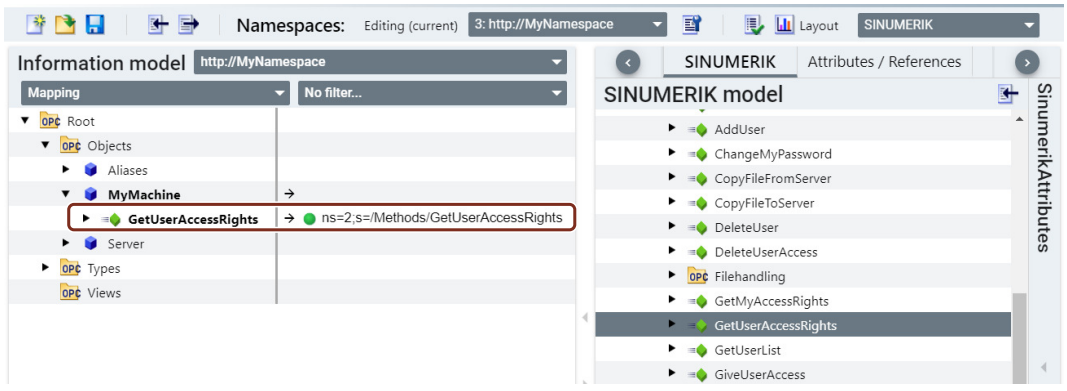


Figure 4-17 SINUMERIK method added

Adding a new instance variable and mapping the method from SINUMERIK tab

To add a new instance for a method, follow the below steps:

1. Under "Objects" node, right-click on "MyMachine" node and then click on "Add Instance".

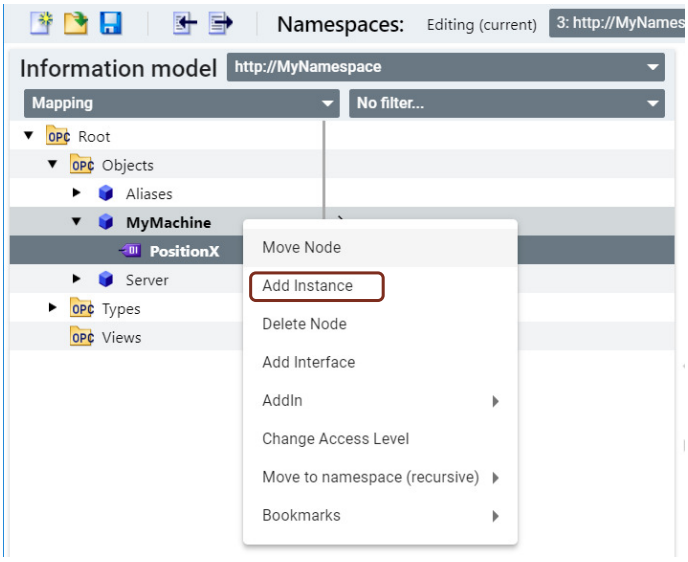


Figure 4-18 Adding a new instance for a method

2. The "Add Instance" popup window appears. Enter a name in the "Name" field.
3. Select "Method" from the "NodeClass" drop-down list and click "Ok".

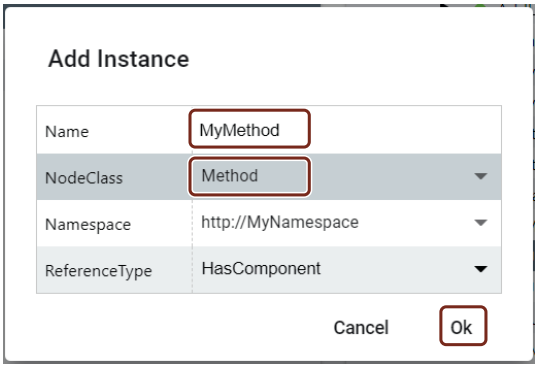


Figure 4-19 Add Instance popup for a method

4. The new instance is added for a method under "MyMachine" node. Expand the "MyMethod" node.

5. Right-click on "InputArguments" node and then click on "Add New Argument".

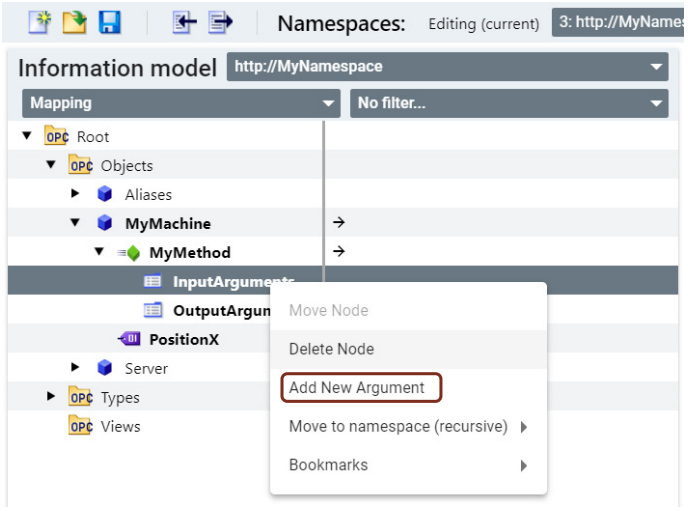


Figure 4-20 Adding a new argument under method

6. Select the newly created argument and then configure the values in the "Attributes / References" tab according to the method argument.

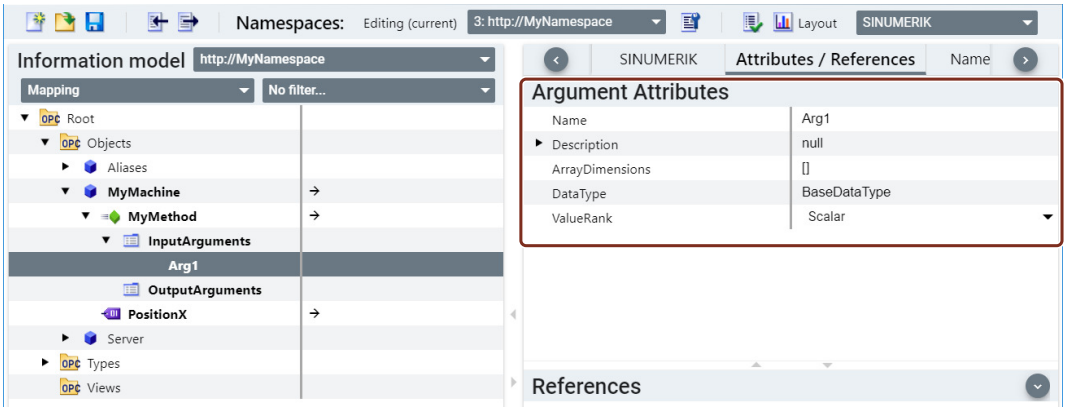


Figure 4-21 Arguments tab

7. Then right-click on "OutputArguments" node and then click on "Add New Argument".

8. Select the newly created argument and then configure the values in the "Attributes / References" tab according to the method argument.
9. Drag and drop the method from the "SINUMERIK" tab to the "MyMethod" node in the "Information model" tab as shown in the below image.

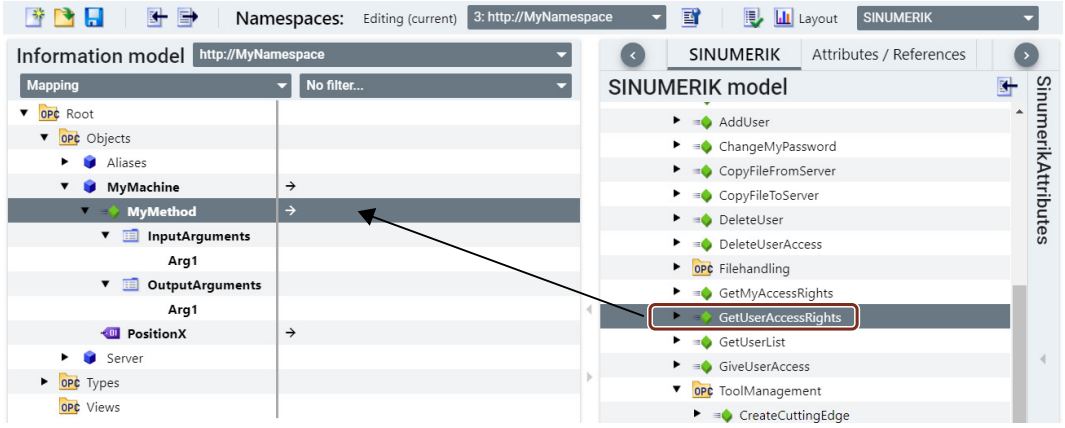


Figure 4-22 Mapping SINUMERIK method

The method is mapped in the mapping table in the "Information model" tab.

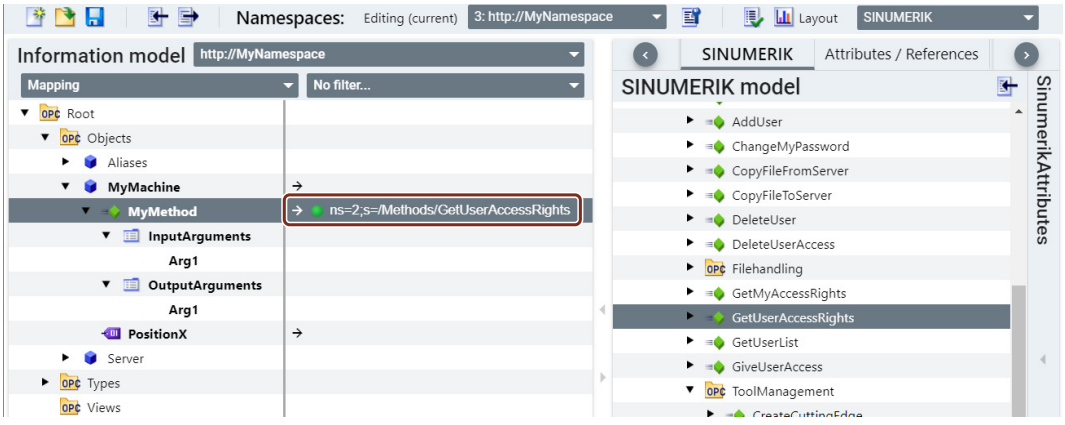


Figure 4-23 SINUMERIK method mapped in mapping table

Adding a new instance for an alarm

To add a new instance for an alarm, follow the below steps:

1. Under "Objects" node, right-click on "MyMachine" node and then click on "Add Instance".

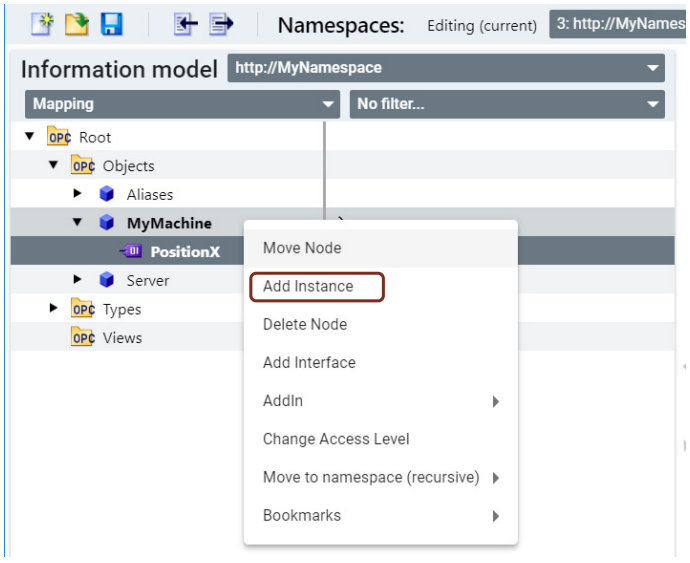


Figure 4-24 Adding a new instance for an alarm

2. The "Add Instance" popup window appears. Enter a name in the "Name" field.
3. Select "Object" from the "NodeClass" drop-down list and then click "Ok".

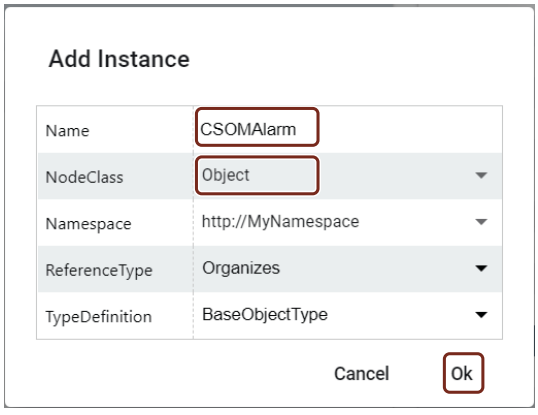


Figure 4-25 Add Instance popup for an alarm

4. The new instance is added for an alarm under "MyMachine" node. Click on "EventNotifier" in the "Additional OPC UA Attributes" tab as shown below.

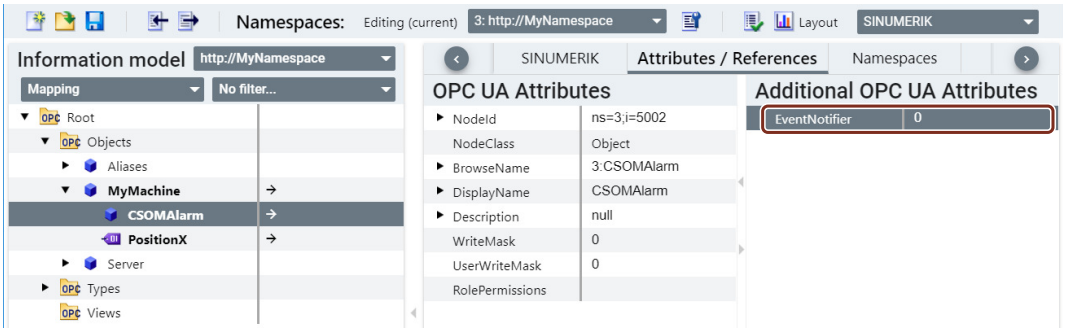


Figure 4-26 New Instance added under a variable for alarm

5. The "Event Notifier" popup window appears. Select "SubscribeToEvents" check-box and click "Ok".

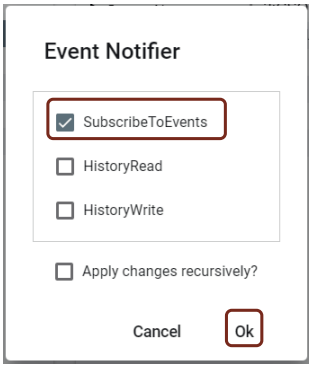


Figure 4-27 Event Notifier popup for an alarm

Result

An object with event notifier is created and can be used for subscribing alarms. There is no need for any mapping from SINUMERIK node.

Adding file system node in CSOM

Before adding a file system node, you need to do the following changes in the settings page in SiOME:

1. Click icon in the SiOME home page and then click "Settings" as shown in the below image.
2. The "Settings" popup window appears. Change the highlighted fields as shown in the below image and then click "Ok". The settings are applied.

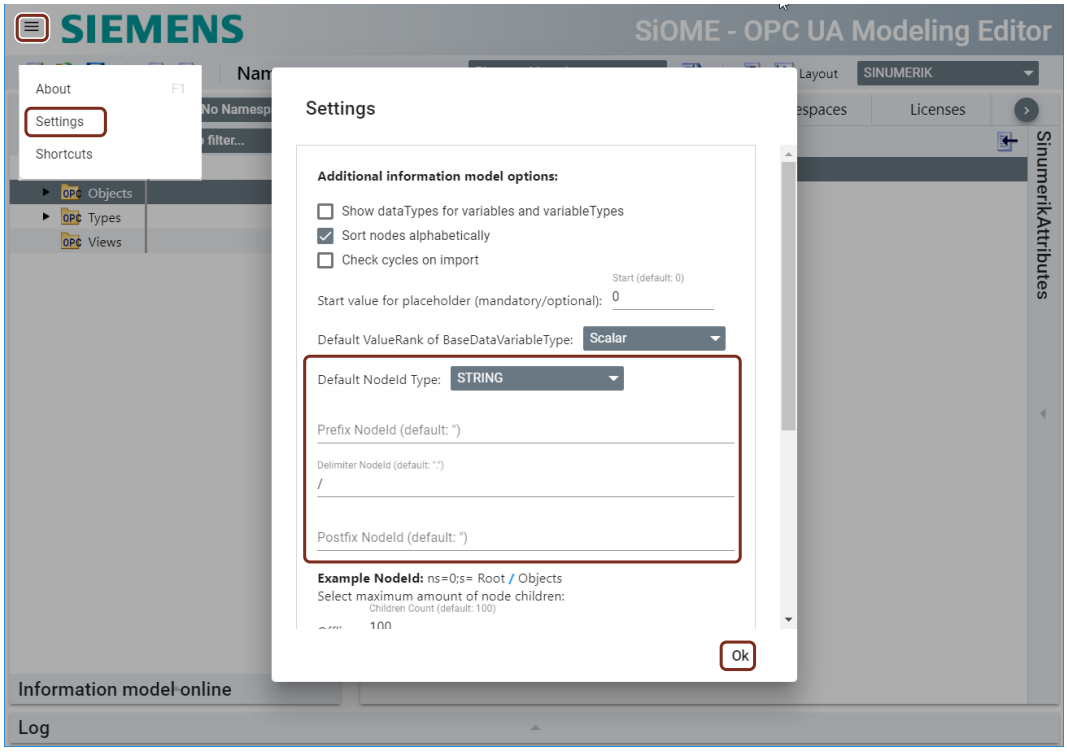


Figure 4-28 SiOME Settings page

To add a file system node, follow the below steps:

1. Click on "Please add or choose a namespace" and then click "Add New Namespace" as shown in the below image.
2. The "Add Namespace" popup window appears. Enter a name in the "Namespace URI" field and then click "Ok".

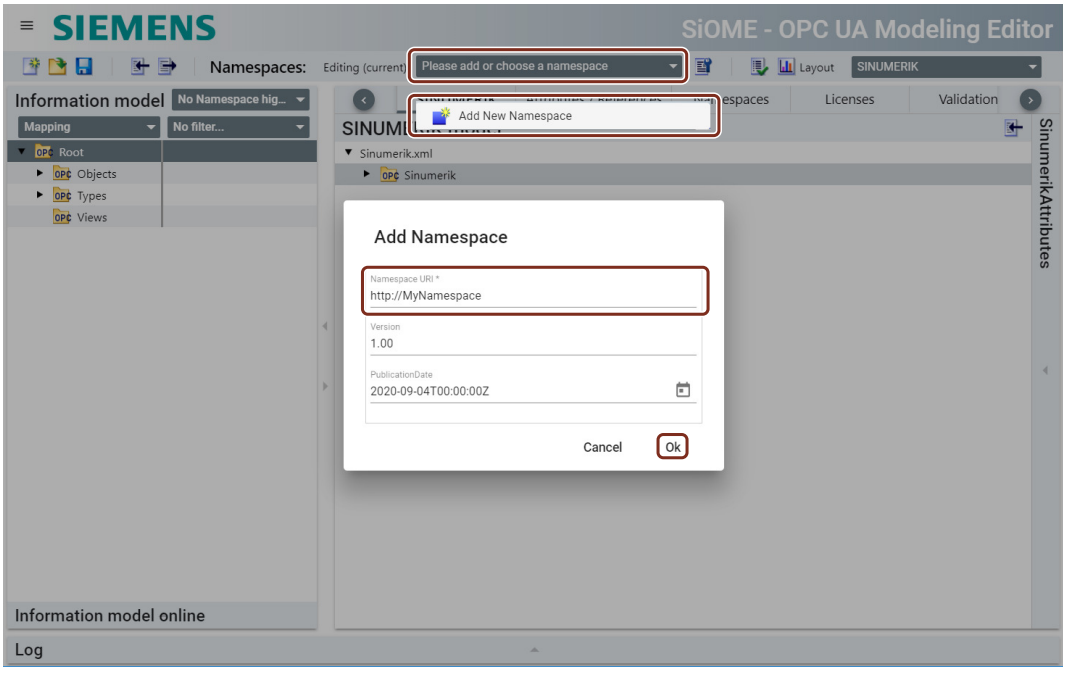


Figure 4-29 Namespaces tab

3. The new namespace is added in "Namespaces" tab. Right-click on "Objects" node in "Information model" tab and then click on "Add Instance".

4. The "Add Instance" popup window appears. Enter a name in the "Name" field.

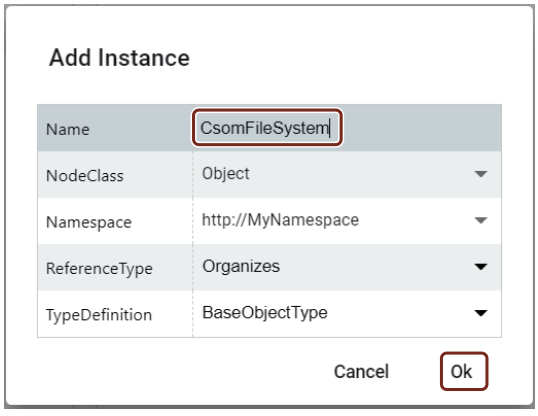


Figure 4-30 Add Instance popup window

5. Verify that newly added namespace is selected in the "Namespace" row and then click "Ok". The new instance is added under "Objects" node.

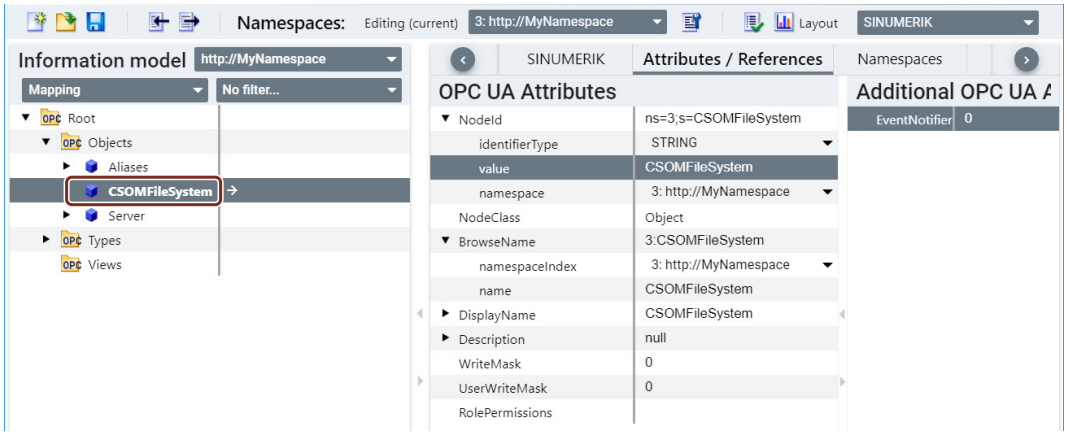


Figure 4-31 New instance is added under object node

Adding a SINUMERIK file directory under file system node

SINUMERIK file directory node can be added in two ways:

- Direct drag and drop under parent node.
- Manually adding a new node of folder type/file directory type under parent node.

Direct drag and drop under parent node

1. To add a SINUMERIK file directory under custom object, press and hold the **ctrl** button and drag and drop the required SINUMERIK file directory from the "SINUMERIK" tab to the "CsomFileSystem" node as shown in the below image.

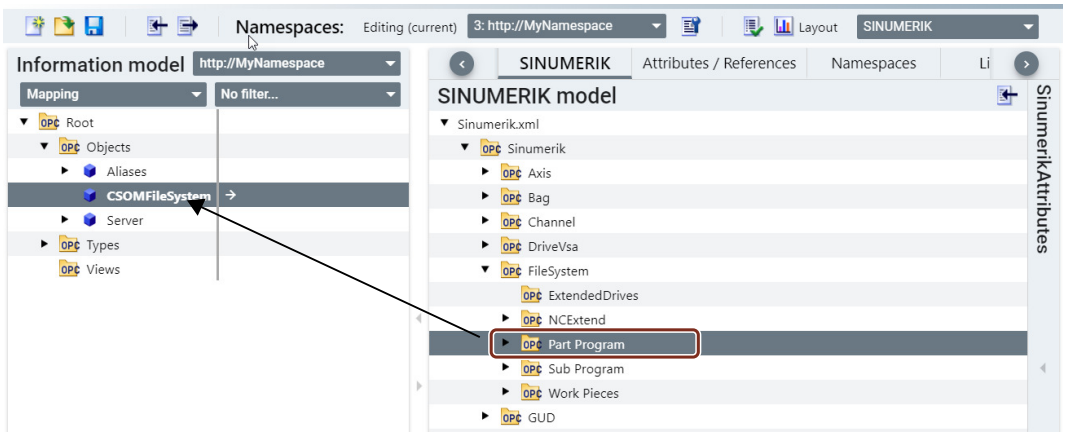


Figure 4-32 Direct drag and drop under custom object

2. The SINUMERIK file directory is added under parent node.

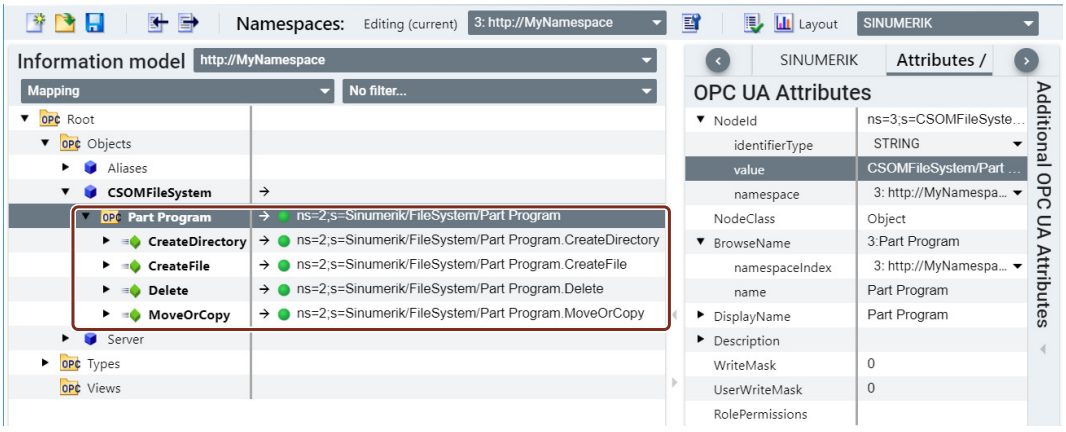


Figure 4-33 SINUMERIK file directory added under parent node

Note

This method is also applicable if you want to add the complete SINUMERIK file system node. See the below image for more information.

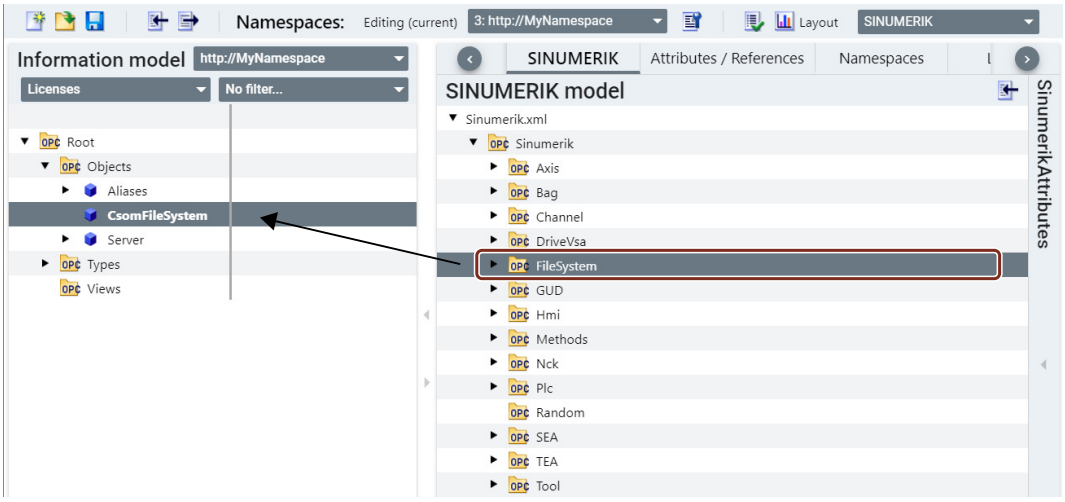


Figure 4-34 Adding complete SINUMERIK file system node

Manually adding a new node of folder type/file directory type under parent node

1. Under "Objects" node, right-click on "CsomfileSystem" node and then click on "Add Instance".
2. The "Add Instance" popup window appears. Enter a name in the "Name" field.
3. Select "FolderType" or "FileDirectoryType" from the "TypeDefinition" drop-down list and then click "Ok".

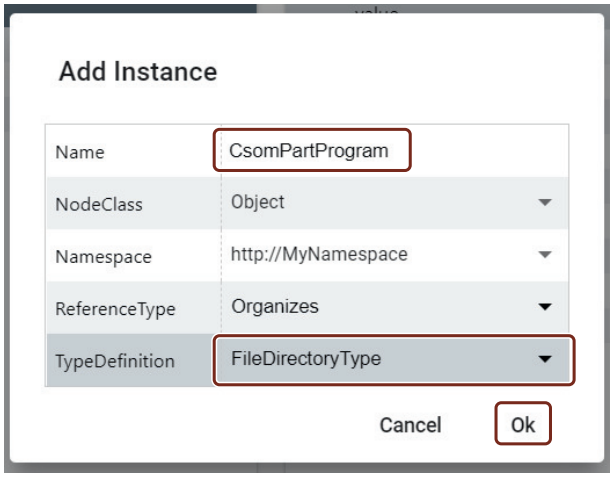


Figure 4-35 Add instance popup_File System

4. The new instance (here "CsomPartProgram") is added under "CsomfileSystem" node.

Note

Under file system node, except extended drives, all other nodes of file system should be of file directory type.

5. Drag and drop the required SINUMERIK file system directory from the "SINUMERIK" tab to the "CsomPartProgram" node as shown in the below image.

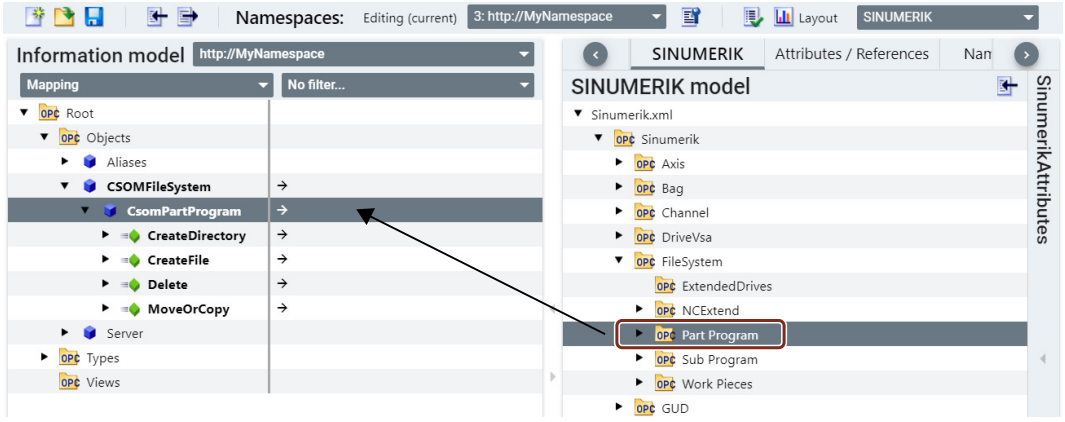


Figure 4-36 Adding a new node of file directory type under custom object

6. The "CsomPartProgram" node is mapped in the mapping table.

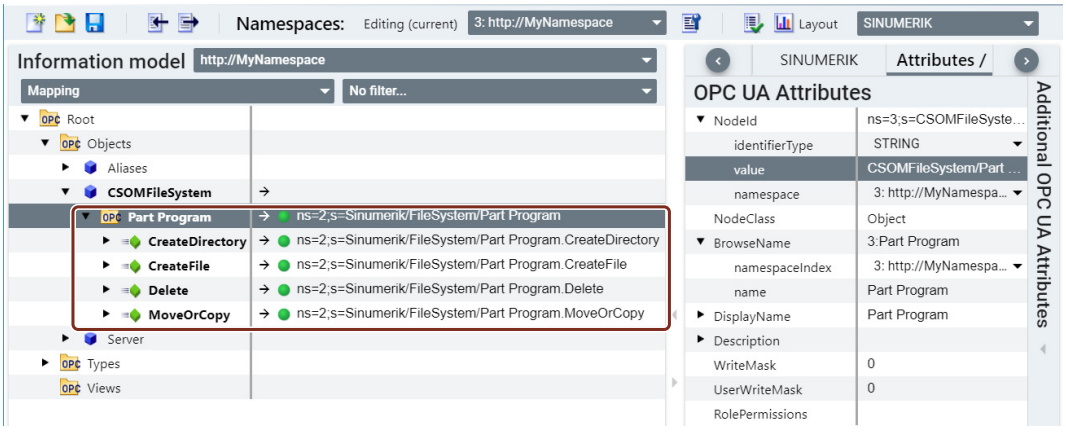


Figure 4-37 SINUMERIK file directory added under custom object

4.3.3.4 Option management in SiOME

Overview

License management is used to enable the availability of nodes within an existing information model based on licenses. These licenses can be used for machine models based on the machine manufacturers need or end user requirements. Any SINUMERIK variable (PLC/NCK) variable can be used by the machine manufacturer to enable the license functionality based on machine model. With the license's functionality user will have a flexibility of displaying different variables and methods according to the license set. Therefore, the SINUMERIK OPC UA Server supports two new use cases in conjunction with a CSOM:

- Individualization of the information model for modular machines on runtime level.
- Allowing a machine manufacturer to make information available within the OPC UA Server at runtime depending on whether a customer has bought a license or not.

This is basically done by engineering licenses within SiOME. To follow an easy to implement solution a "license" is basically any NC / PLC variable (can be chosen freely) in the SINUMERIK system which needs to have a certain value (can be defined in SiOME).

Following are the benefits with license functionality:

- Flexibility to use a single custom model for different machine models
- Flexibility to use a single custom model by OEM for different users
- Flexibility to add the required data set as part of custom model
- Reducing time for both commissioning and creating different models by OEM
- Lot of time can be saved while modeling and maintenance

Adding a license

To enable license options in custom models, follow the below steps:

1. Click "Layout" drop down and select "SINUMERIK". The SINUMERIK layout is displayed.
2. Under "Licenses" tab, click on **+** icon to add licenses, as shown in the below image.

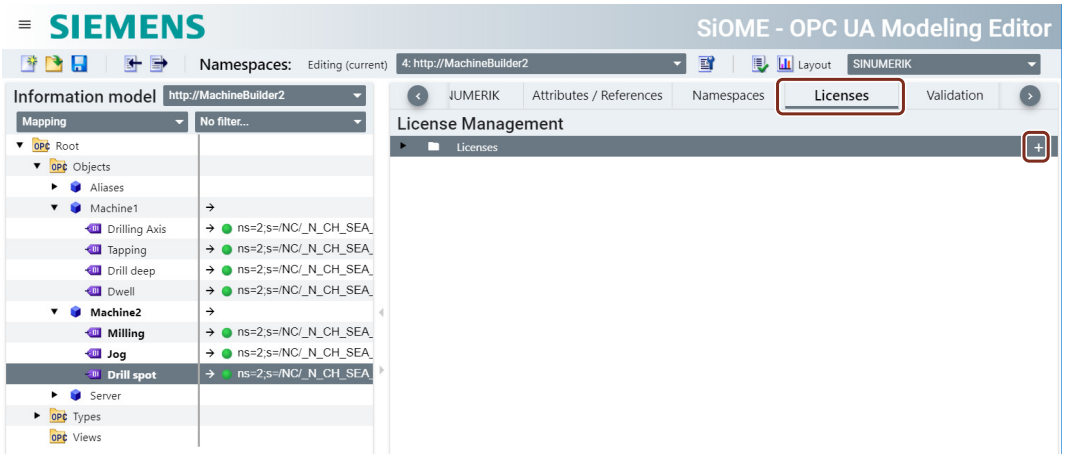


Figure 4-38 Adding licenses in custom models

3. An information popup window appears. By clicking "Ok", a new namespace will be created automatically for SINUMERIK license.

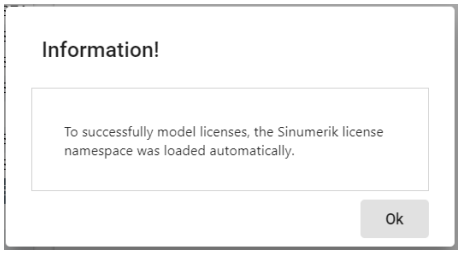


Figure 4-39 Licenses namespace popup window

Note

The SINUMERIK license namespace will get the next available namespace number.

4. The "Add license" popup window appears. Make the necessary settings as described in the below table.

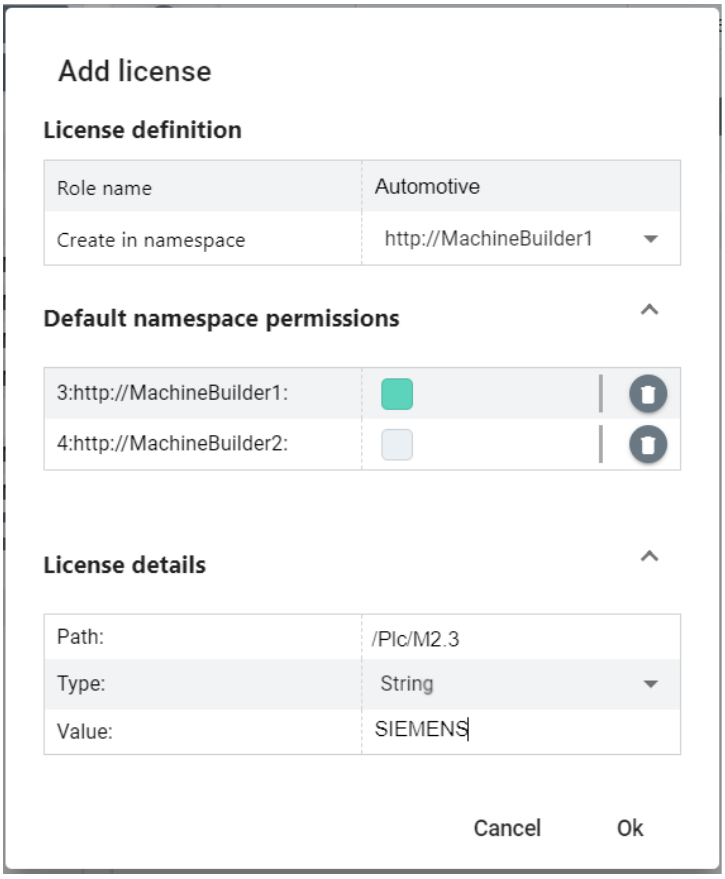


Figure 4-40 Add license popup

Group	Settings	Description	Example
License definition	**Role name**	You can edit the name of the license.	
	Create in name-space	Select the namespace for which you want to add the license from the drop down.	
Default namespace permissions		Select the default namespace. Sets the default license to the selected namespace. If a namespace is selected here, all variables of this namespace will be part of this licence by default. If this is not required, then do not select any-thing. It is also possible to deselect the name-space by clicking again on the selection field. Green color indicates, selected and White color indicates, not selected. To remove the selected namespace, click icon.	

Group	Settings	Description	Example
License details	**Path**	Enter the path of the license variable. It is basically the path of the variable within the standard information model of the SINUMERIK node within the OPC UA Server.	Absolute addressing "/Plc/M2.3" Symbolic addressing "/Plc/Memory/activatelicense"
	Type	Select the data type from the drop down list.	String
	Value	Select or enter the value depending on the data type selection. If the variable has the same values as entered here, then the part of the OPC UA browse tree will be available in the OPC UA server, after restart.	"SIEMENS"

Note

The "Value" set for each license should match with the value in specified "Path" during the Operate/HMI startup. In case of mismatch in value, the variables/methods associated with the license will not be displayed in OPC UA address space.

5. Click "OK". The license is added, as shown in the below image.

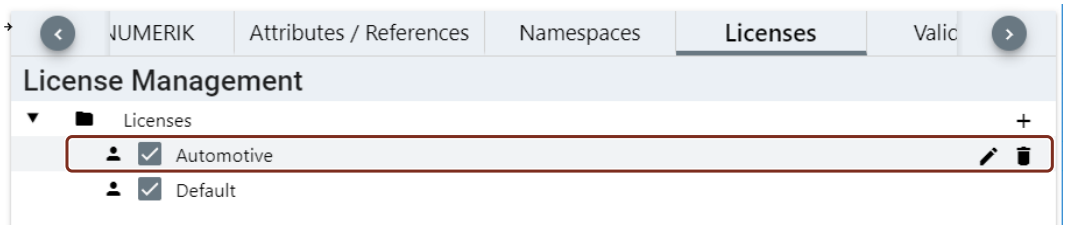


Figure 4-41 License added

If you want to edit the license details, then click icon. If you want to remove the license, then click icon. Add more licenses in the same way, if you need.

Note

SINUMERIK OPC UA server supports up to 20 licenses.

6. Select "Licenses" from the drop down, as shown in the below image.

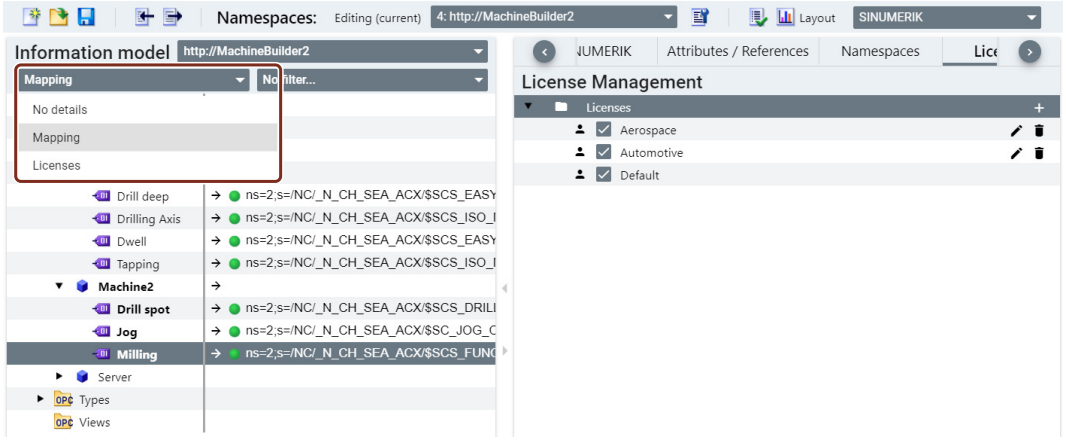


Figure 4-42 Switching from mapping to licenses

Setting licences for CSOM namespaces

1. Assign the newly created licenses to the variables as per the requirement. The variables in the "Default" license will always be shown in the address space.

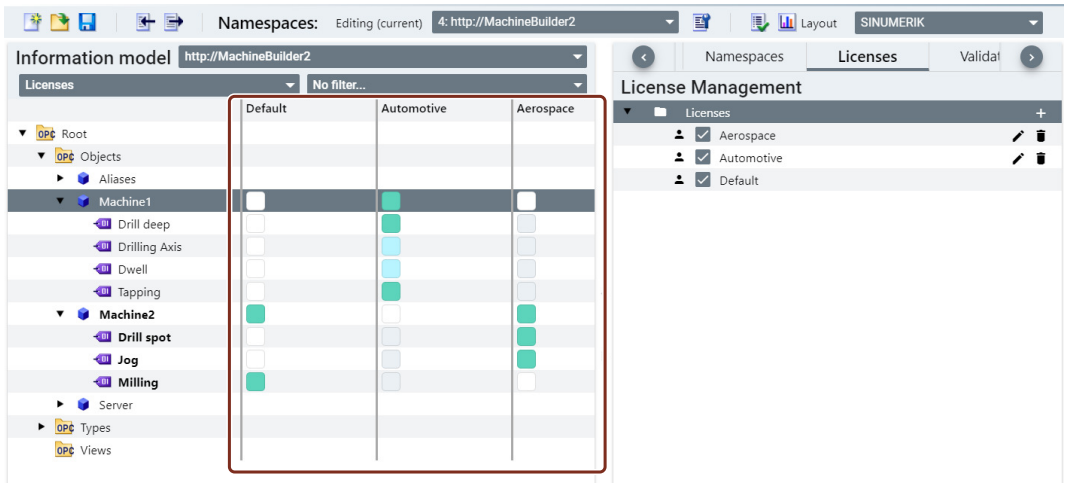


Figure 4-43 Assigning the licenses to variables

Note

After a license is set, restart of the OPC UA Server is required to update the browse tree.

After assigning the licenses to the variables, export the CSOM (XML) as mentioned in the next topic.

4.3.3.5 Exporting CSOM (XML)

To export the CSOM (XML) to your local machine, follow the below steps:

1. Click the Export XML icon as shown in the below image.

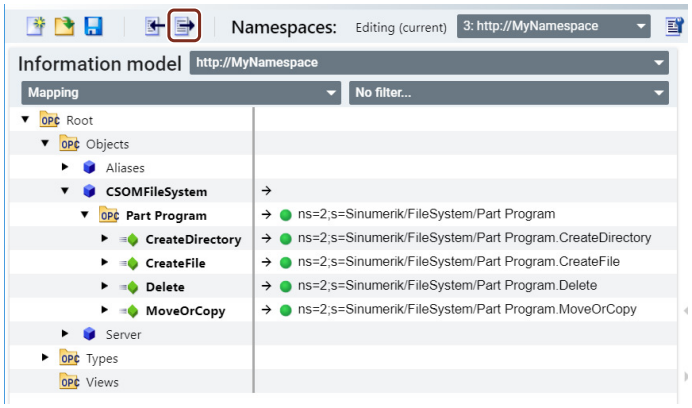


Figure 4-44 Exporting the CSOM

2. The "Export XML" popup appears. Click on browse icon.

3. A "Save as" dialog box appears.
   Select the location to save the exported CSOM (XML) file and then click "Save".

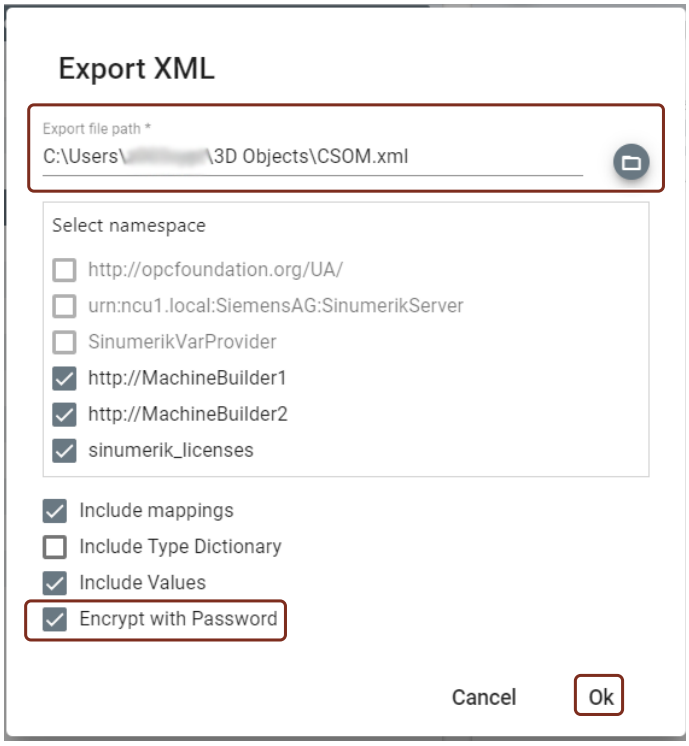


Figure 4-45 Export XML popup

4. If you want to encrypt the CSOM file, then select "Encrypt with Password" check box.
5. Click "OK". A password popup appears.

6. Enter a password. Also remember the password because it is required while converting the CSOM from XML to binary in SINUMERIK Access MyMachine/ P2P.

Note

Passwords must always contain a combination of upper-case and lower-case letters as well as at least one number and one special character. Password must comprise at least eight characters.

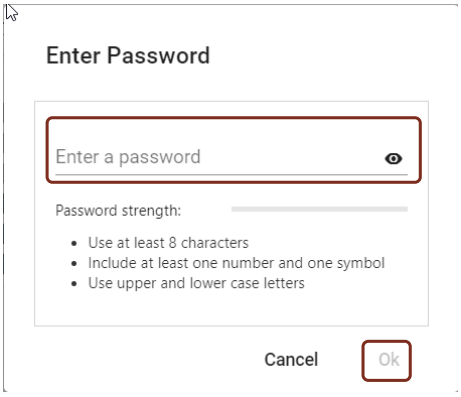


Figure 4-46 CSOM XML encrypt with password popup

7. Click "OK". The CSOM (XML) file is saved in the specified location.

For further steps, continue with the chapter Converting the CSOM from XML to binary (Page 73).

For a more detailed description of SiOME, refer to Industry Online Support (https://support.industry.siemens.com/cs/de/en/view/109755133). You can find a function manual, download link, further explanations and applications examples on modeling and mapping.

Additional information on data types, modeling rules and necessary user access rights for the modeling process are explained in the following chapters:

- Mapping data types (Page 70)
- Modeling rules (Page 71)
- Access control with CSOM (Page 72)

4.3.3.6 Mapping data types

Mapping data types

The table below shows the compatible SINUMERIK data type for each OPC UA data type.

Assign the data types as shown below (SINUMERIK data type – OPC UA data type). Other assignments are not permitted. You are responsible for the rule-compliant selection and assignment of the data types.

You may find **further information** on mapping of OPC UA data types in the document "OPC UA Information Model for IEC 61131-3".

Table 4-1 Mapping of data types

SINUMERIK data type	OPC UA data type
Bool	Boolean
Character	Byte
Byte	Byte
Word	UInt16
Short Integer	SByte
Doubleword	UInt32
Long Integer	Int64
Float	Float
Real	Float
Double	Double
String	String

Note

The PLC datatype doubleword (e.g. DBD, MD) can be used for datatype “DInt” or “Real”.

For getting “Real” values via OPC UA it is necessary to append the “REAL” specifier to the PLC variable used in the mapping, e. g.: DB100.DBD5:REAL.

4.3.3.7 Modeling rules

Following are the rules while modeling the exported SINUMERIK model (XML) with SiOME:

- The exported SINUMERIK Model (XML) should not be used in the "Information Model" window as a base for model creation.
- No new nodes should be added under the below namespaces:
  - 0: http://opcfoundation.org/UA/
  - 1: urn:ncu1.local:SiemensAG:SinumerikServer
  - 2: SinumerikVarProvider
- Up to 10.000 nodes (over all CSOM namespaces) can be modeled within the OPC UA server.
- Total namespaces should not be more than 10 (Including the above namespaces).
- First three namespaces 0, 1 and 2 should not be edited, deleted or change in order.
- Standard folder or file functions names should not be renamed.
- Standard folder or file functions argument should not be modified.
- No new Objects, Variables or Methods should be added under standard folder or file structures.
- Standard folder or files should not be deleted under standard folder or file structures.

- Additional namespaces should have an index of 3 or higher.
- In SiOME, when a new node is created with a "ValueRank" set to "Dimension" then the value attribute of the node should be initialized by clicking on the "Value" in the "Attribute" window.

Note

If customer model is not shown in the browse tree, then refer to the error logs under the folder (..\user\sinumerik\hmi\log\opcua).

4.3.3.8 Access control with CSOM

For the CSOM, the customer has the following possibilities to provide access rights for variables:

1. In SiOME, the CSOM Access level can be defined.
2. In addition, the OPC UA administrator has two new access rights:
   - CsomReadx
   - CsomWritex

To read a variable within a CSOM namespace the OPC UA administrator has to provide the user with the access right "CsomReadx" while "x" stands for the namespace index.

For example, to read a variable out of namespace 3, the user only needs to get the access right "CsomRead3". No other access rights are needed. The same is valid for "CsomWritex".

The following table gives an overview about the interaction between CSOM access level and access rights of target device. A variable that is read only by access rights of target device can not be written by OPC UA, even if the OPC UA access write is read/write (3).

Table 4-2 Access table

CSOM AccessLevel	CSOM namespace rights	Rights of target device	Result
1 = Read	No access	Read / Write	No access
	Read	Read / Write	Read
	Write	Read / Write	No access
	Read / Write	Read / Write	Read
2 = Write	No access	Read / Write	No access
	Read	Read / Write	No access
	Write	Read	No access
	Write	Read / Write	Write
	Read / Write	Read	No access
	Read / Write	Read / Write	Write

CSOM AccessLevel	CSOM namespace rights	Rights of target device	Result
3 = Read/Write	No access	Read / Write	No access
	Read	Read / Write	Read
	Write	Read	No access
	Write	Read / Write	Write
	Read / Write	Read	Read
	Read / Write	Read / Write	Read / Write

4.3.4 Converting the CSOM from XML to binary

The exported CSOM (XML) from SiOME needs to be converted to a binary format that can be read by SINUMERIK OPC UA server. The converted binary file has a more compact format and is therefore controller optimized. For this conversion process SINUMERIK Access MyMachine/ P2P is used.

The following graphic shows the process of converting the CSOM (XML) to binary format.

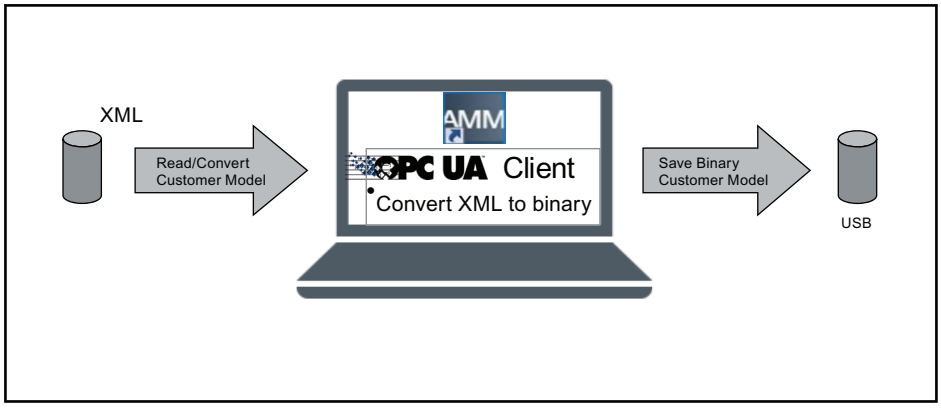


Figure 4-47 Converting the CSOM from XML to binary

Procedure

1. Open the application "SINUMERIK Access MyMachine /P2P".
2. Click "Tools > Sinumerik Opcua Server Tools > Model Binary Converter". A popup window appears.

3. Select the location of the XML file under "Input XML File" and specify the location to save the binary file under "Output BIN File".

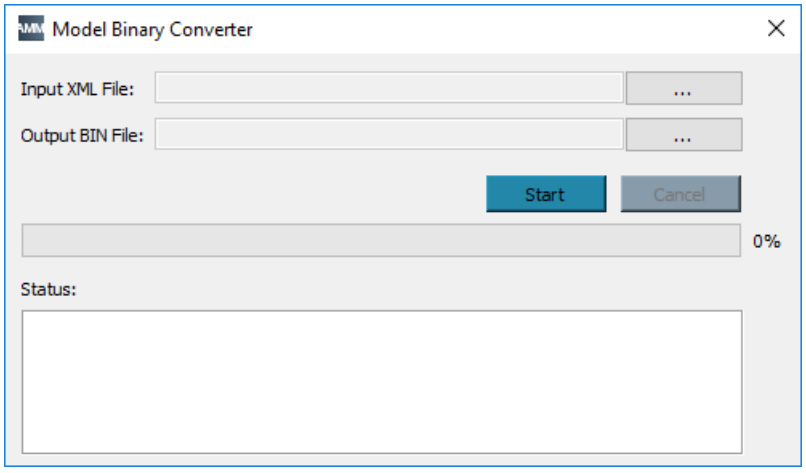


Figure 4-48 Model Binary Converter

4. Click "Start" button to generate the binary file. If the XML file is encrypted, then a password popup appears.

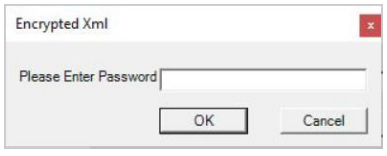


Figure 4-49 Password popup

5. Enter the same password that was set while encrypting the exported CSOM (XML) file from SiOME.
6. Click "OK". If the password is correct, then the binary file will be generated and saved in the specified location.

Result

Imported CSOM XML file is converted to binary format.

4.3.5 Importing the CSOM into the SINUMERIK OPC UA server

After converting the CSOM (XML) to a binary format, it can be imported to the SINUMERIK OPC UA server.

The following image shows the process of importing the CSOM (binary format) to SINUMERIK OPC UA server.

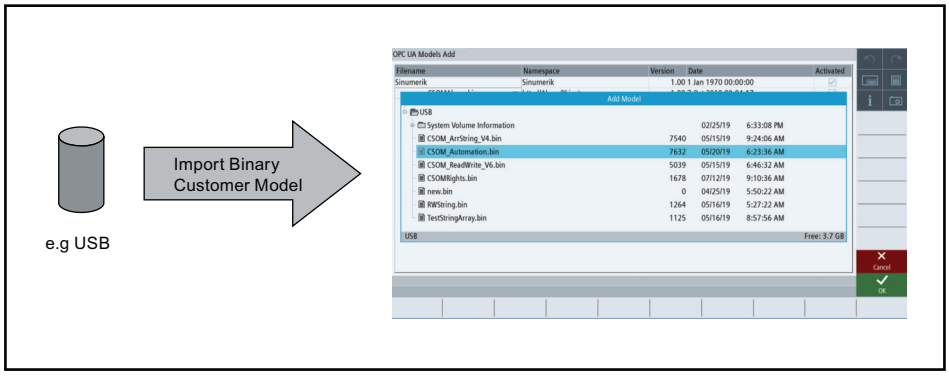


Figure 4-50 Importing the CSOM into the SINUMERIK OPC UA server

Procedure

1. Copy the binary file either to an USB/Networkshare or - alternatively - transfer the file via AMM directly to the control.
   - "**\user\sinumerik\hmi\opcua\models**" for NCU
   - "**C:\Program Files (x86)\Siemens\Motion Control\user\sinumerik\hmi\opcua \modeles**" for PCU/IPC

   Note

   If models folder is not present, then create a folder name **models.**

2. Press the softkey "Add Model" in the OPC UA model dialog and select the saved binary file.
3. Press the softkey "OK".
   The model is visible in the OPC UA model dialog.
4. Then press the softkey "Change" and activate the customer specific model.
5. Restart the OPC UA server by restarting SINUMERIK OPC UA server.

Result

The CSOM is now accessible in SINUMERIK Operate.

Note

For accessing data via an OPC UA client, it is necessary to have appropriate access rights (see chapter "List of access rights").

See also

List of access rights (Page 86)

4.4 CSOM dialog in SINUMERIK Operate

4.4.1 Overview

To have a comfortable way to work with a customer specific object model, the OPC UA dialog offers a special section, which can be found under the softkey "Model".

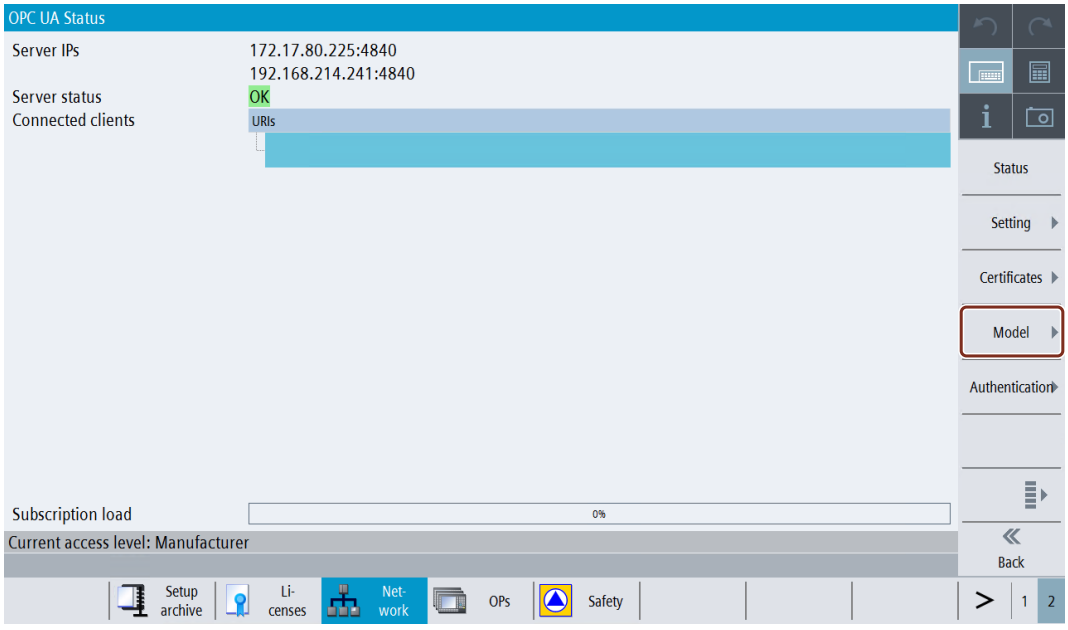


Figure 4-51 Softkey Model

The SINUMERIK Operate dialog has the following functionality:

- Import of CSOM binary file from USB/Networkshare or via AMM
- Display the filename of the selected binary file
- Deleting the selected binary file
- Activate the selected binary file
- Deactivate the actual binary file

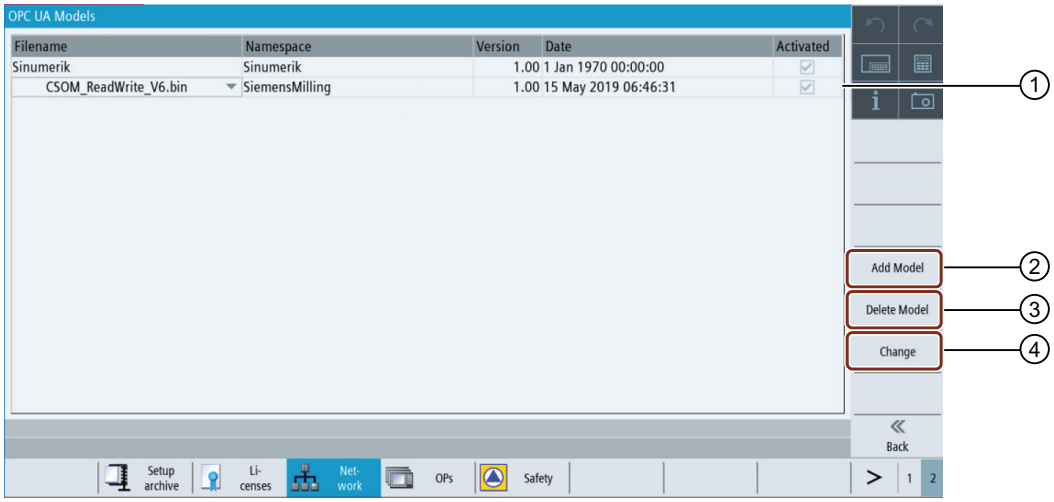
Note

The changes are visible only after restarting the OPC UA server.

4.4.2 OPC UA model dialog

Overview

Press the "Model" softkey to get the below screen.



① The OPC UA model dialog shows the activated CSOM and also displays the following information:

- Filename of the CSOM
- The namespace of the CSOM
- The version of the CSOM
- The date of the import
- Status of activation

② You can add new CSOM

③ You can delete the CSOM

④ You can change the CSOM by selecting from the drop down list and also it can be activated/ deactivated

Figure 4-52 OPC UA Models

4.4.3 Adding model

Note

This option can be seen with user access rights, but the user can add models with only manufacturer's access rights.

Procedure

1. To add a customer specific object model, press the softkey "Add Model".

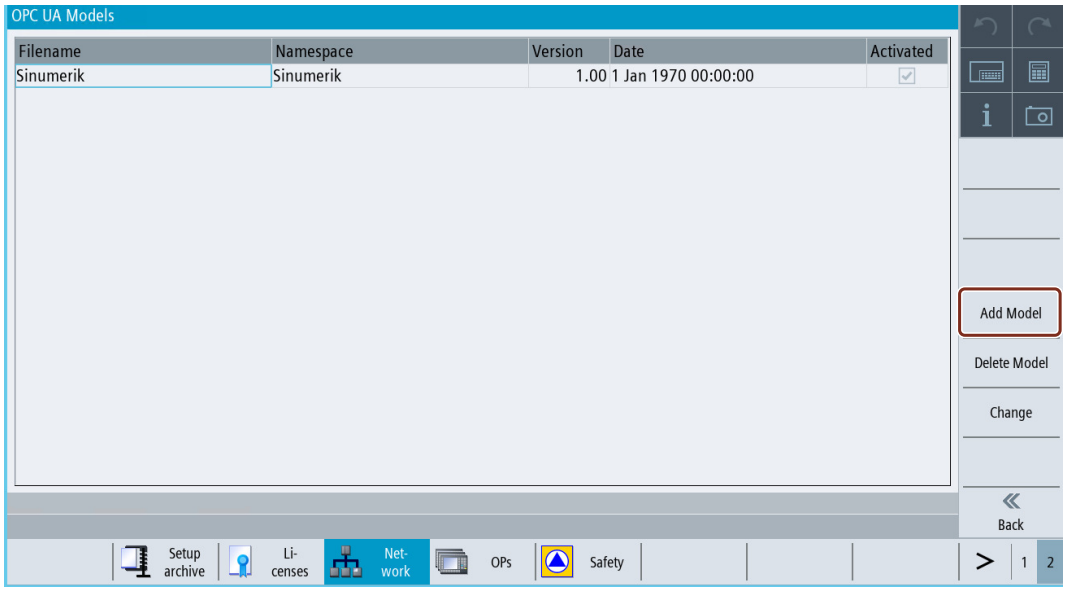


Figure 4-53 Softkey Add Model

The "Add Model" popup screen appears.

2. Select the binary file from either USB/Networkshare.

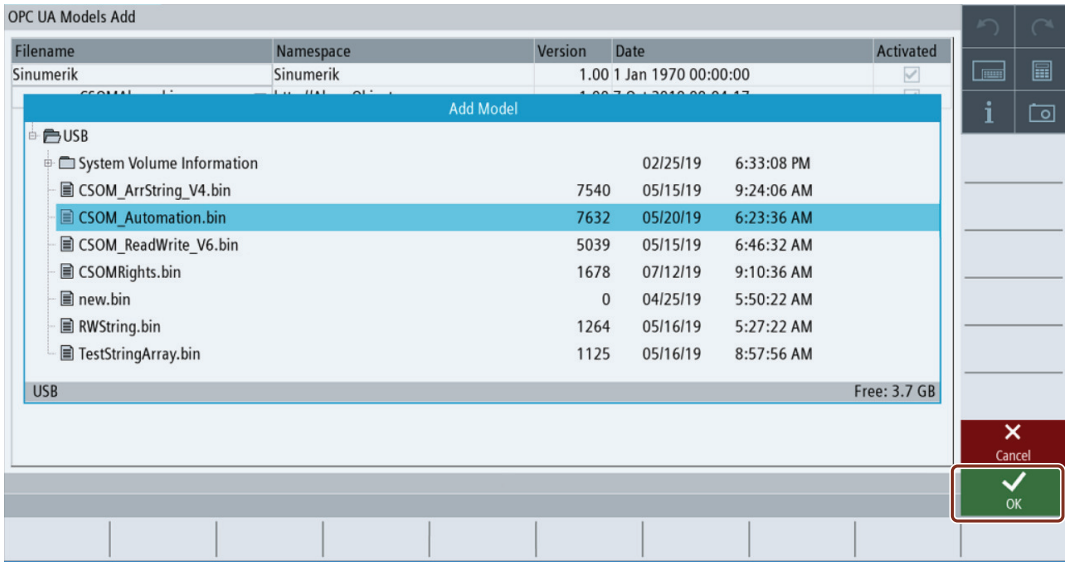


Figure 4-54 OPC UA Models Add

Pressing the softkey "Cancel" will do no action and return to "OPC UA Models" screen.

Pressing the softkey "OK" will add the binary file.

4.4.4 Deleting OPC UA model

Procedure

1. To delete a customer specific object model press the softkey "Delete Model".

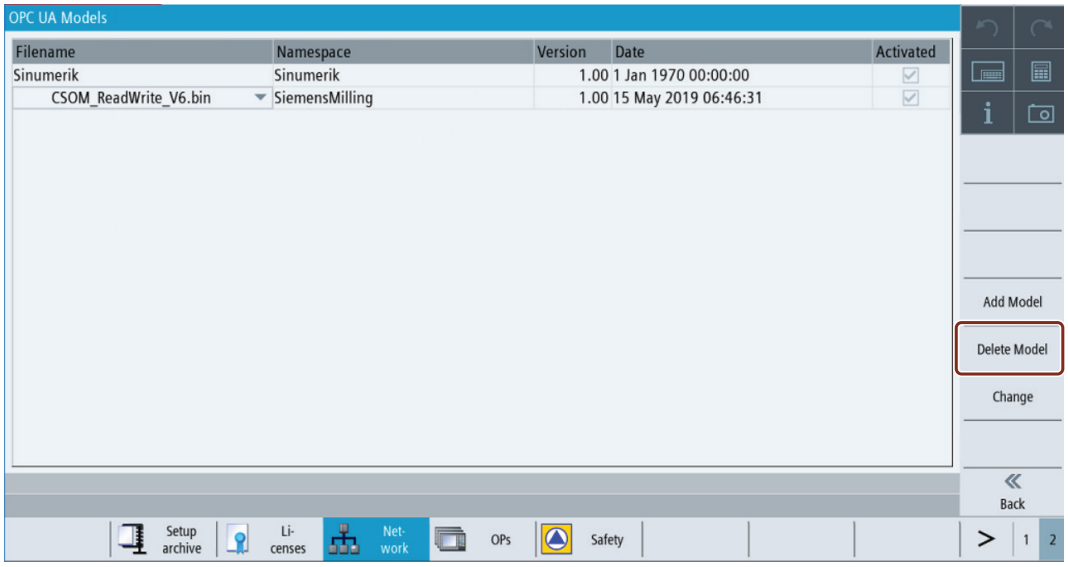


Figure 4-55 Softkey Delete Model

2. Select the model you want to delete from the CSOM drop-down list and then click "OK".

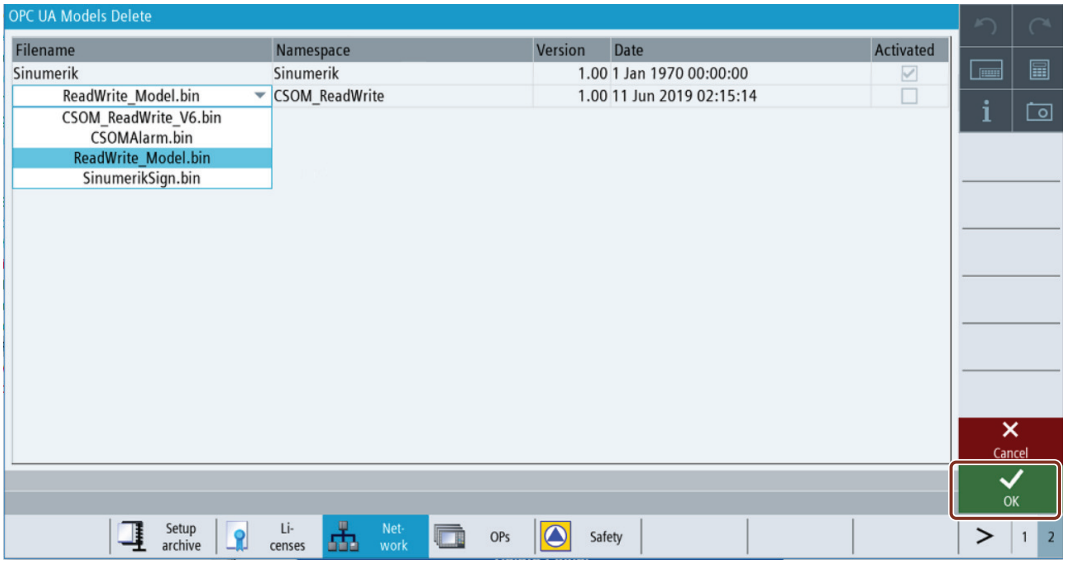


Figure 4-56 OPC UA Models Delete

A pop-up screen will appear asking you for confirmation of deletion:

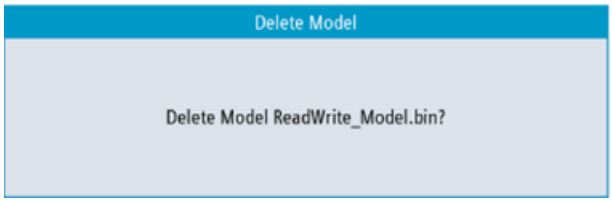


Figure 4-57 Delete Model popup

Pressing the softkey "Cancel" will do no action and return to "OPC UA Models" screen.

Pressing the softkey "OK" will delete the customer model.

4.4.5 Activating / Deactivating OPC UA model and SINUMERIK namespace

Procedure

1. Press the softkey "Change".

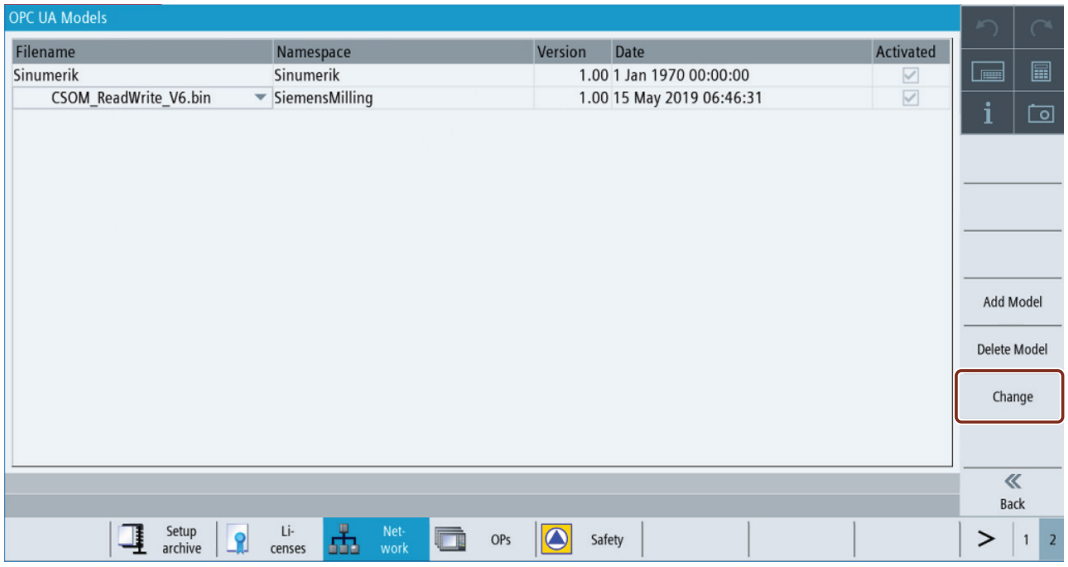


Figure 4-58 Softkey Change

2. The following screen appears where you can perform the following functions:
   - Selecting the CSOM file from the drop-down list.
   - Activating the CSOM file by selecting the check box.
   - Deactivating the CSOM file by clearing the check box.
   - Activating the SINUMERIK namespace by selecting the check box.
   - Deactivating the SINUMERIK namespace by clearing the check box.

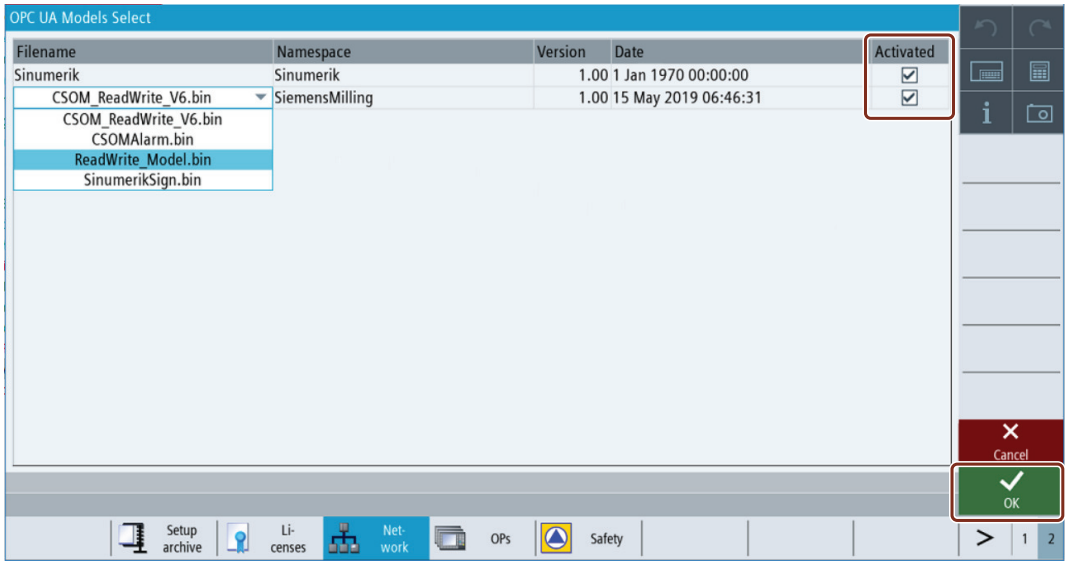


Figure 4-59 OPC UA Models Select

Pressing the softkey "Cancel" will do no action and return to "OPC UA Models" screen.

Pressing the softkey "OK" will apply the changes.

User administration

5

5.1 Overview

The admin can add/delete users and access rights via OPC UA methods provided by the server. Therefore a connection with a generic client must be established, using the admin credentials.

Users and access rights can then be assigned using the following OPC UA server methods:

- Add users (AddUser, AddCertificateUser)
- Delete users (DeleteUser)
- List users (GetUserList)
- Change password (ChangeMyPassword)
- Give access rights (GiveUserAccess)
- Remove access rights (DeleteUserAccess)
- List access rights (GetMyAccessRights, GetUserAccessRights)

NOTICE
Misuse of access rights As an administrator, you are fully responsible for the administration of users and their access rights. Any error in the administration process can lead to the misuse of access rights.

Note

Anonymous connection

You can also establish an anonymous connection during commissioning, if this setting is active, but the methods will not be available (feedback: "BadRequestNotAllowed").

Note

Anonymous user

Anonymous users don't have any access (Read/Write) rights after installation. As an administrator, you have to set these access rights explicitly.

Note

Administrator has only read rights

Note that the administrator has only read rights per default. Other rights need to be set explicitly.

Note

You can only add or remove users or access rights if you are connected as administrator. If you call the methods with a different user, you will receive the message "BadInvalidArgument".

5.2 User management

A new user created with the "AddUser" or "AddCertficateUser" function has no access rights at all. The user administrator has the responsibility for the user management and the associated access rights. All users must use a secure password.

Table 5-1 Methods for user administration

Method	Description	
AddUser	Creates a new user for accessing OPC UA. **Input arguments:**	
	UserName	User Name
	Initially, the password of the new user is the user name. It should then be changed using the method "ChangeMyPassword".	
AddCertificateUser	Creates a new user for accessing OPC UA via certificate authentication. **Input arguments:**	
	UserName	user, certificate is issued to
	CertficateData	Certificate(.der) as byte string
DeleteUser	Deletes a user who was added previously using the method "AddUser" and "AddCertificateUser". **Input arguments:**	
	UserName	User Name
	The administrator user, created when OPC UA was set up, cannot be deleted.	
GetUserList	The administrator can read the list of all users. **Input arguments:**	
	-	List of users
ChangeMyPassword	Changes the password for the **connected** user. **Input arguments**:	
	OldPwd	Current password
	NewPwd1	New password
	NewPwd2	New password (security prompt)
	Important! Whereas the methods "AddUser", "DeleteUser", "GiveUserAccess" and "DeleteUserAccess" can only be called up if the user is connected as the administrator, the user must connect as the corresponding user in order to change the password.	

5.3 Access rights management

After setting up the OPC UA components, the administrator user has read access to all data ("SinuReadAll") but no write access. These access rights must be set explicitly.

The administrator can also add the user access rights for individual PLC DBs.

Table 5-2 Methods for user administration

Method	Description	
GetMyAccessRights	The currently **connected** user can read his access rights. **Input Arguments:**	
	-	Rights
GetUserAccessRights	The administrator can read the access rights of another user. **Input Arguments:**	
	User name	Rights
DeleteUserAccess	Deletes the specified access rights for a user. **Input Arguments:**	
	User	A user whose access rights are to be deleted
	Realm	The access rights to be deleted as a string. If a user wants to delete several access rights, they must be separated by a semicolon.
For all possible realm strings, see chapter "List of access rights". Example: DeleteUserAccess("John","PlcReadDB100") Admin wants to delete read rights of user "John" for PLC data block DB100.		

Major access rights versus minor access rights

A possibility to reset all user access rights is to use the general OPC UA access rights behaviour that by deleting a major access right all minor access rights will be deleted too. So if you have granted several read rights for special users to read certain data blocks beforehand, you can reset all of these access rights by deleting "SinuReadAll".

See also

List of access rights (Page 86)

5.4 List of access rights

Below is the list of access rights a user is assigned:

Table 5-3 List of access rights

Method	Description	
GiveUserAccess	Sets the specified access rights for a user. The access rights below can be combined in any combination. **Input Arguments:**	
	User	User name which is to given the access rights
	Realm	The access rights to be set as a string. If a user wants to set several access rights, they must be separated by a semicolon.
	Some possible realm strings are:	
	"StateRead"	Status data - NC, channel, axis, read access
	"StateWrite"	Status data - NC, channel, axis, write access
	"FrameRead"	Zero offsets, read access
	"FrameWrite"	Zero offsets, write access
	"SeaRead"	Setting data, read access
	"SeaWrite"	Setting data, write access
	"TeaRead"	Machine data, read access
	"TeaWrite"	Machine data, write access
	"ToolRead"	Tool and magazine data, read access
	"ToolWrite"	Tool and magazine data, write access, Tool management methods
	"DriveRead"	Drive data, read access
	"DriveWrite"	Drive data, write access
	"GudRead"	User data, read access
	"GudWrite"	User data, write access
	"FsRead"	File system, read access
	"FsWrite"	File system, write access
	"PlcRead"	PLC, read access
	"PlcWrite"	PLC, write access
	"AlarmRead"	Allows to subscribe to alarms
	"RandomRead"	Random, read access
	"RandomWrite"	Random, write access
	"SinuReadAll"	All of the read access operations mentioned
	"SinuWriteAll"	All of the write access operations mentioned
	"ApWrite"	Allows to call method "Select"
	"PlcReadDBx"	PLC DB read access (x indicates the DB number)
	"PlcWriteDBx"	PLC DB write access (x indicates the DB number)
	"CsomReadx"	CSOM read access (x indicates the namespace number, possible numbers: 3-9)[1]
	"CsomWritex"	CSOM write access (x indicates the namespace number, possible numbers: 3-9)[1]
	Examples: • GiveUserAccess ("MyUser", "GudRead; PlcWrite") Sets the read access for user data for the "MyUser" user and sets the write access for the PLC.	

Method	Description
	• GiveUserAccess ("John","PlcReadDB100") Admin gives read rights to user "John" for PLC data block DB100.

[1] CSOM read and write access rights is sufficient to access the CSOM namespace. It overwrites all the other user rights. Therefore, no other additional rights are needed for reading or writing in CSOM address space (for example, PLC read access rights is not needed to read the PLC data in CSOM).

Note

CSOM access is not covered by SinuReadAll / SinuWriteAll, but must be assigned individually.

5.5 Changing access rights for OPC UA configuration screens in SINUMERIK Operate

It is possible for the machine manufacturer to change the access rights for the OPC UA server configuration screens according to the protection level of the configuration.

Therefore the machine builder can change the access level needed to change, for example, the authentication information for the admin or the CSOM within the OPC UA server.

The access rights for OPC UA configuration screens in SINUMERIK Operate can be adjusted in the following path:

- for NCU "*/card/user/sinumerik/hmi/opcua/cfg/opcuiaccess.conf*"
- for PCU/IPC "*C:\Program Files (x86)\Siemens\MotionControl/user/sinumerik/hmi/opcua/cfg/opcuiaccess.ini*"

Note

Bear in mind that changing access rights can allow the customer to change essential configurations of the OPC UA server, especially gaining access to variables that the machine manufacturer may not want to offer.
Access rights for the SINUMERIK Operate screens can only be changed with the manufacturer's access rights.

Procedure

1. Open the file "opcuiaccess.conf" on your embedded controller.
2. Change the access right for the desired OPC UA functionality. The access rights mirror the SINUMERIK Operate access levels from 1 to 7.

Access level	Protected by	Area
1	Password: SUNRISE (default value)	Manufacturer
2	Password: EVENING (default value)	Service
3	Password: CUSTOMER (default value)	User
4	Keyswitch 3	Programmer, machine setter
5	Keyswitch 2	Qualified operator
6	Keyswitch 1	Trained operator
7	Keyswitch 0	Semi-skilled operator

3. Save the file again.

Functionality

6

6.1 Overview

Overview

The OPC UA server provides the possibility to communicate with SINUMERIK via OPC UA. The following functionalities of the OPC UA specification are supported by the server:

- **Data Access:**
  Read, write and subscribe to SINUMERIK variables (NC, PLC)
- **Alarms & Conditions:**

  Event based provision of SINUMERIK alarms and messages from HMI, NC and PLC
- **Methods:**
  User management, file transfer, tool management and program selection

This chapter describes the address space of the OPC UA server and gives further information how to address some SINUMERIK specific values. Especially since a lot of SINUMERIK values are stored in arrays or matrices.

Furthermore you can find description on the SINUMERIK alarm object and how to get the alarms from the server.

At the end of this chapter explanation on how users can transfer files from or to the server using the SINUMERIK file system.

6.2 Address space model

Address space model

If the OPC UA server is browsed, the available address space is mapped under the "Sinumerik" node.

Global User Data (GUD) can be found under the "/Sinumerik/GUD" node.

The PLC blocks (inputs, outputs, bit memory, data blocks) can be found under the "/Sinumerik/Plc" node.

Machine data can be found under the node "/Sinumerik/TEA".

Setting data can be found under the node "/Sinumerik/SEA".

Observe the following while browsing:

- In the address space of the NC, the displayed variables always represent only the first parameter of the corresponding unit.
  Example:
  The R parameters can be found under "Sinumerik > Channel > Parameter > R". The corresponding identifier is called "/Channel/Parameter/R", which is finally mapped to "/Channel/Parameter/R[u1, 1]". If you want to access other parameters, you need to specify the corresponding index in brackets, e. g. "/Channel/Parameter/R[u2,56]".
- In the address space of the PLC, the displayed variables represent the access format that has to be extended accordingly.
  Example:
  The variable "/Plc/MB" is in the address space and is mapped to "/Plc/MB0". For accessing further bytes this variable must be extended by the appropriate byte number, e.g. "/Plc/MB6".
- The address space of the NC also contains variables that are not available in a corresponding machine configuration. These variables return "BadAttributeIdInvalid" as value.

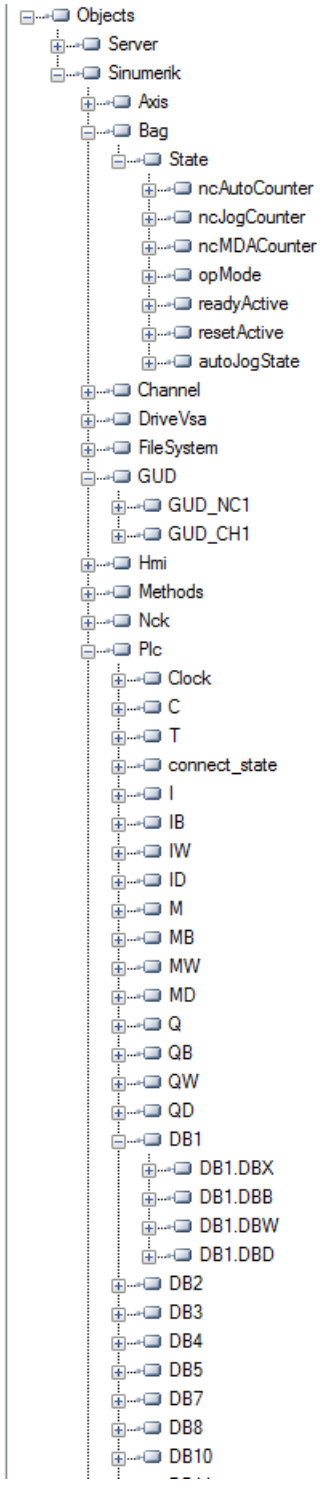


Figure 6-1 Browsing

6.3 Variable access

6.3.1 Variable paths for NC access operations

Note

You have to pay attention to the correct upper-case and lower-case of the "nodeID". The respective identifier of the "nodeID" provides information on the correct notation.

Variable access

The variable paths for NC access are stored in the address space of the SINUMERIK Operate OPC UA server.

You can obtain **further information** from the List Manual for 840D sl and 828D "NC variables and interface signals" (https://support.industry.siemens.com/cs/de/en/view/109769139).

Attribute	Value
NodeId	NodeId
NamespaceIndex	2
IdentifierType	String
Identifier	/Channel/Parameter/R
NodeClass	Variable
BrowseName	2, "/Channel/Parameter/R"
DisplayName	"en_us", "R"
Description	"en_us", "R"
WriteMask	0
UserWriteMask	0
Value	
SourceTimestamp	1/30/2014 3:17:25.822 PM
ServerTimestamp	1/30/2014 3:17:25.822 PM
SourcePicoseconds	0
ServerPicoseconds	0
Value	66
DataType	Double
NamespaceIndex	0
IdentifierType	Numeric
Identifier	11
ValueRank	-1
ArrayDimensions	BadAttributeIdInvalid
AccessLevel	Readable, Writeable
UserAccessLevel	Readable, Writeable
MinimumSamplingInterval	50
Historizing	false

Figure 6-2 Identifier for R parameter

The displayed NC variables always represent only the first parameter of the corresponding NC data area (channel, TO area, mode group).

Example

Syntax of the R parameter is as follows: R[Channel,Parameter]

The R parameters are found under the identifier "/Channel/Parameter/R", which is eventually mapped to "/Channel/Parameter/R[u1, 1]". If you want to access other parameters, you must correspondingly extend the identifier, for example "/Channel/Parameter/R[u2, 56]".

Table 6-1 Examples of variable paths (NC access operations)

Variable path	Description
/Channel/Parameter/R[u1,10]	R parameter 10 in channel 1
/Channel/Parameter/R[u1,1,5] /Channel/Parameter/R[u1,1,#5]	R parameter array R parameters 1 to 5 in channel 1
/Channel/GeometricAxis/name[u2,3]	Name of the 3rd axis in channel 2
/Channel/GeometricAxis/actToolBasePos[u1,3]	Position of the 3rd axis in channel 1

Note

Please keep in mind that with array access only max 149 parameters are allowed in one access operation (for example /Channel/Parameter/R[u1, 1, #149]).

6.3.2 Variable paths for GUD access operations

GUD variables can be found in the OPC UA server under the "/Sinumerik/GUD" node.

The displayed GUD variables always represent only the first parameter (for GUD arrays) of the first NC channel (for channel-dependent GUD variables). If you want to access a different parameter of a GUD array or a different channel, you must extend the identifier accordingly for the NC access.

GUD arrays are 1-indexed for access, and access is always one-dimensional. This means, the index must be calculated for multi-dimensional arrays.

Example 1: One-dimensional array, NC-global GUD array

"UGUD.DEF" file

```
DEF NCK INT ARRAY[2]
M17
```

Access is performed as follows:

```
ARRAY[0] → /NC/_N_NC_GD3_ACX/ARRAY[1]
ARRAY[1] → /NC/_N_NC_GD3_ACX/ARRAY[2]
```

Example 2: Two-dimensional array, channel-dependent GUD array

"UGUD.DEF" file

```
DEF CHAN INT ABC[3,3]
M17
```

Access is performed as follows:

```
ABC[0,0] → /NC/_N_CH_GD3_ACX/ABC[u1, 1]
ABC[0.1] → /NC/_N_CH_GD3_ACX/ABC[u1, 2]
ABC[0.2] → /NC/_N_CH_GD3_ACX/ABC[u1, 3]
ABC[1.0] → /NC/_N_CH_GD3_ACX/ABC[u1, 4]
ABC[1.1] → /NC/_N_CH_GD3_ACX/ABC[u1, 5]
ABC[1.2] → /NC/_N_CH_GD3_ACX/ABC[u1, 6]
ABC[2.0] → /NC/_N_CH_GD3_ACX/ABC[u1, 7]
ABC[2.1] → /NC/_N_CH_GD3_ACX/ABC[u1, 8]
ABC[2.2] → /NC/_N_CH_GD3_ACX/ABC[u1, 9]
```

6.3.3 Variable paths for PLC access operations

PLC variables can be found in the OPC UA server under the "/Sinumerik/Plc" node.

In the address space of the PLC, the displayed variables represent the access format that has to be extended accordingly.

Example

Syntax of the PLC variable is as follows: "/Plc/MB"

This variable must be extended by the appropriate byte number, e.g. to "/Plc/MB6".

Note

On SINUMERIK 828D, you can only access the freely definable customer data blocks from DB9000.

Access formats

The various access formats are shown in the following table. They need to be prefixed with "/Plc/".

Note

The data type is converted during access with the OPC UA data access interface. Refer to the following table for the data type conversions.

Table 6-2 PLC syntax

Area	Address (IEC)	Permissible data types	OPC UA data type
Output image	Qx.y	**BOOL**	Boolean
Output image	QBx	**BYTE**, CHAR, STRING	UInt32 String
Output image	QWx	**WORD**, CHAR, INT,	UInt32 Int32

Area	Address (IEC)	Permissible data types	OPC UA data type
Output image	QDx	**DWORD**, DINT, REAL	UInt32 Int32 Double
Data block	DBz.DBXx.y	**BOOL**	Boolean
Data block	DBz.DBBx	**BYTE**, CHAR, STRING	UInt32 String
Data block	DBz.DBWx	**WORD**, CHAR, INT	UInt32 Int32
Data block	DBz.DBDx	**DWORD**, DINT, REAL	UInt32 Int32 Double
Input image	Ix.y	**BOOL**	Boolean
Input image	IBx	**BYTE**, CHAR, STRING	UInt32 String
Input image	IWx	**WORD**, CHAR, INT	UInt32 Int32
Input image	IDx	**DWORD**, DINT, REAL	UInt32 Int32 Double
Bit memory	Mx.y	**BOOL**	Boolean
Bit memory	MBx	**BYTE**, CHAR, STRING	UInt32 String
Bit memory	MWx	**WORD**, CHAR, INT	UInt32 Int32
Bit memory	MDx	**DWORD**, DINT, REAL	UInt32 Int32 Double
Counters	Cx	-	Byte
Timers	Tx	-	UInt32
PLC time	Clock	-	UInt16

Notes regarding the table:

- "x" represents the byte offset; "y" the bit number in the byte and "z" the data block number.
- The data type in bold characters is the default data type and does not have to be specified. The specifications DB2.DBB5.BYTE and DB2.DBB5 are equivalent.
- Square brackets are used to access arrays, e.g. "/Plc/DB5.DBW2:[10]" (word array of length 10).
- Access to STRING arrays ("/Plc/DB123.DBB0:STRING[5]") is not supported.

Examples of variable paths (PLC access operations)

Table 6-3 Examples of variable paths (PLC access operations)

Variable path	Description
/Plc/M5.0	Memory bit 0 at byte offset 5
/Plc/DB5.DBW2	Word (16-bit) at byte offset 2 in data block 5

Variable path	Description
/Plc/DB8.DBB2:STRING	UTF8 string beginning at byte offset 2 in data block 8
/Plc/DB8.DBW2:[10]	Array of 10 words beginning at byte offset 2 in data block 8
/Plc/DB100.DBB1	Byte at byte offset 1 in data block 100
/Plc/DB2.DBD0:REAL[10]	Array of 10 double words (32-bit) beginning at byte offset 0 in data block 2, which are formatted as a floating-point number

Note

- Timers can only be read. A timer is active if it contains a value other than 0.
- If the data type CHAR or STRING is used in conjunction with a byte access, UTF8 characters are read, but if either data type is used in conjunction with a word access, UTF16 characters are read.
- Variables of the STRING type contain the maximum length in the first byte and the actual length in the second byte. When strings are written, the actual length is adapted accordingly. The maximum length is not changed.
- For the STRING data type in conjunction with a byte access (e.g. "/Plc/DB99.DBB0:STRING"), the maximum string length is 255 characters. As a result of the UTF8 formatting, for some characters (e.g. for the "µ"), two bytes are required so that the maximum string length is correspondingly reduced.
- Only one-dimensional arrays are supported.

6.3.4 Variable paths for machine and setting data

The variable paths for machine and setting data are stored in the address space of the OPC UA server under the nodes "/Sinumerik/TEA" and "/Sinumerik/SEA". Pay attention to the correct upper-case and lower-case of the "nodeID". The respective identifier of the "nodeID" provides information on the correct notation.

The displayed machine and setting variables always represent only the first parameter of the corresponding data area (channel, axis).

Table 6-4 Examples of variable paths (machine and setting data)

Variable path	Description
/NC/_N_CH_TEA_ACX/$MC_CHAN_NAME	Channel name of channel 1
/NC/_N_CH_TEA_ACX/$MC_CHAN_NAME[u2]	Channel name of channel 2

Machine data arrays are 1-indexed for access.

6.3.5 Variable paths for 1:N configuration (only target system PCU)

By default, data is accessed on the NCU which is being viewed by SINUMERIK Operate. Switching to a different NCU in the SINUMERIK Operate results in a situation where the OPC UA server is also looking at the value of the now active NCU.

If the access is to be to a specific NCU, the NodeId must be expanded with a prefix:

/Random@<NCUName><NodeId> Examples of variable paths (1:N constellation)

Examples of variable paths (1:N constellation)

Variable path	Description
/Random@NCU_1/Channel/Parameter/R[u1,10] /Random@NCU_2/Channel/Parameter/R[u1,10]	R parameter 10 in channel 1 of NCU_1R parameter 10 in channel 1 of NCU_2
/Random@NCU_1/Plc/DB123.DBB0	Byte at byte offset 0 in data block 123 of NCU_1

Note

The NCU names are listed in the "MMC.ini" file.

Entry:

[GLOBAL]

NcddeMachineNames=NCU1,NCU2

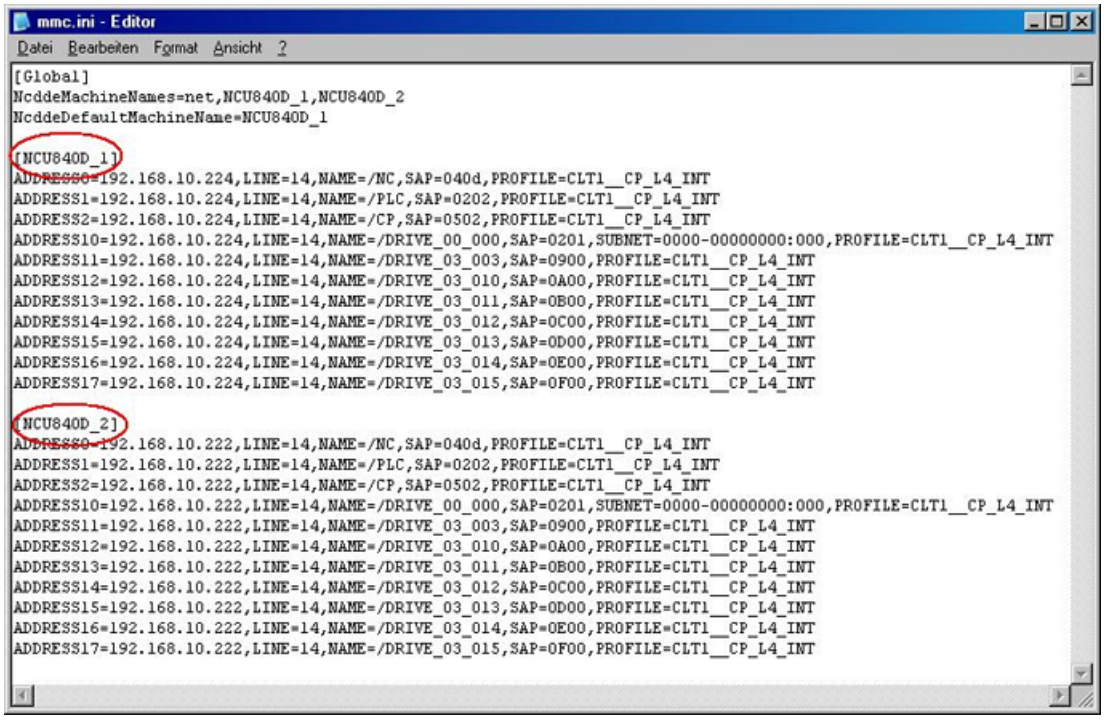


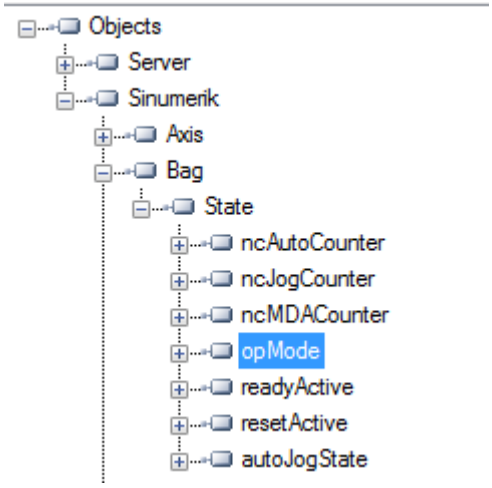
Figure 6-3 NCU names with 1:N

6.3.6 Finding of OPC UA variables

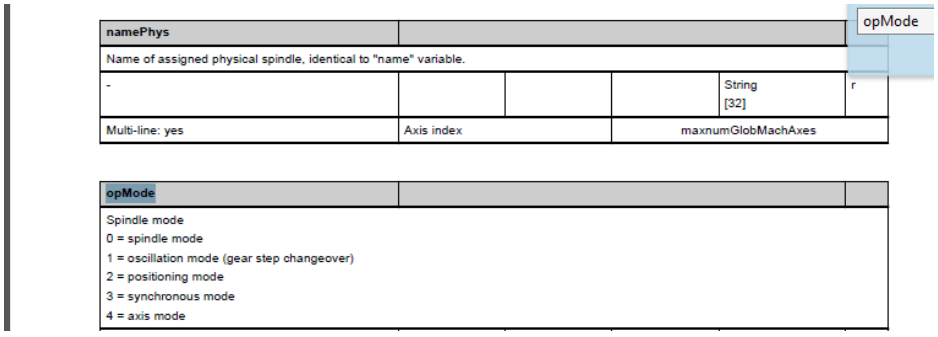
You can find **further information** on variable documentation in the list manual NC variables and interface signals (https://support.industry.siemens.com/cs/de/de/view/109748365/en)

Example 1: Finding an OPC UA variable in the variable documentation

You want to find the variable "opMode" in folder "/Bag/State".

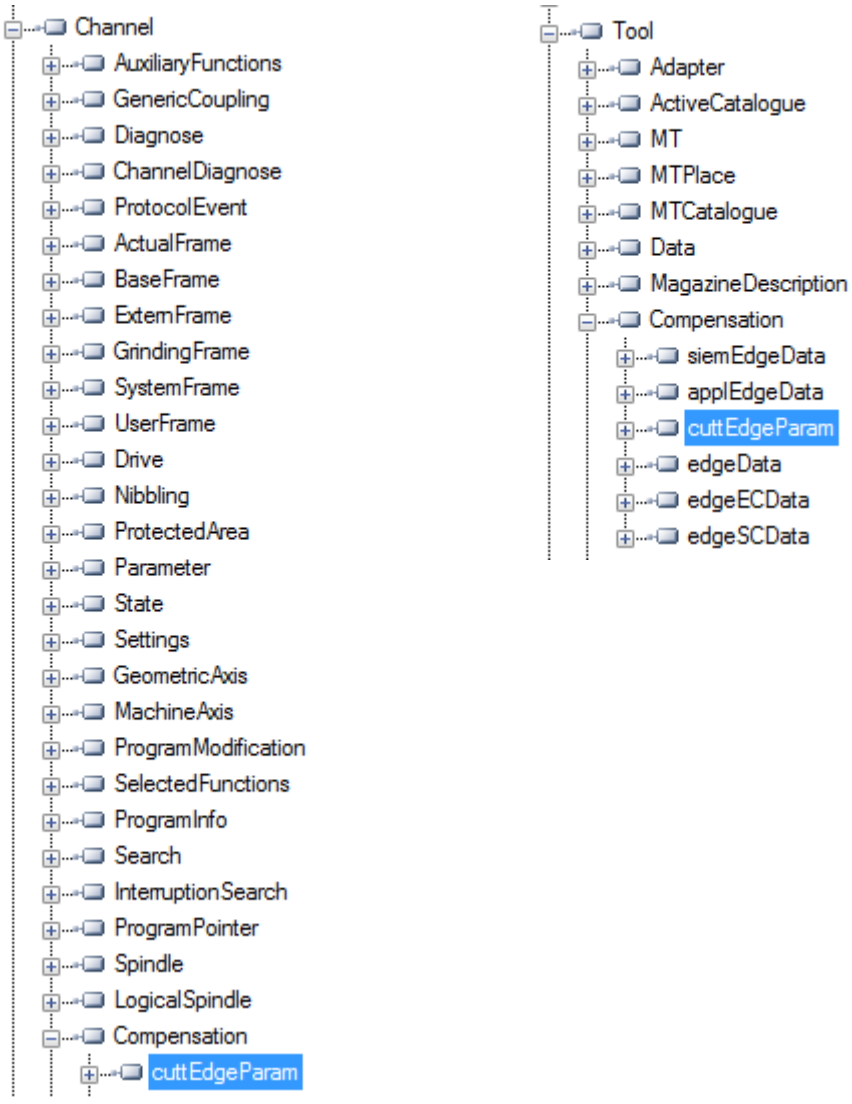


1. Refer to the document mentioned above. Search for "opMode".



Example 2: Finding an OPC UA variable occurring in different folders in the variable documentation

You want to find the variable "cuttEdgeParam" which occurs in the folder "/Channel/Compensation" and "/Tool/Compensation".



1. At the beginning of each chapter for variable sections, you find the information "OEM-MMC: LinkItem" specifying "/ToolCompensation/".

   3.7.2 Area T, Block TO : Tool edge data: Offset data

   OEM-MMC: Linkitem /ToolCompensation/...

   The data module TO is organized as a 2-dimensional variable array.

2. Refer to the document and search for "ChannelCompensation" and then navigate manually to the requested parameter "cuttEdgeParam".

cuttEdgeParam	$TC_DPx[y,z]				
Compensation value parameters for a tool edge					
mm, inch or user-defined	0			Double	wr
Multi-line: Yes	(EdgeNo - 1) * numCuttEdgeParams + ParameterNo		numCuttEdgeParams * numCuttEdges		

Example 3: Finding a variable from documentation on OPC UA client

You want to find the variable "cuttEdgeParam" in the Tool edge data section.

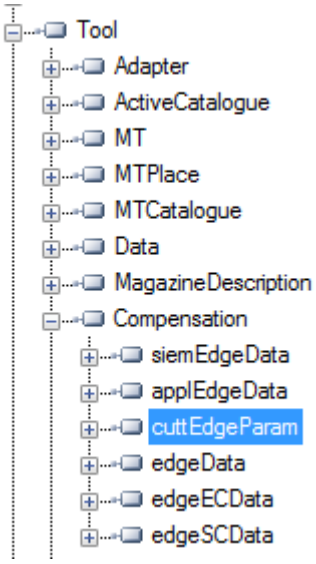
1. At the beginning of each chapter of the variable documentation you find the information "OEM-MMC: LinkItem" specifying here "/ToolCompensation/".

   3.7.2 Area T, Block TO : Tool edge data: Offset data

   OEM-MMC: Linkitem /ToolCompensation/...

   The data module TO is organized as a 2-dimensional variable array.

2. Therefore you will find the variable "cuttEdgeParam" in the OPC UA Browse Tree in the folder "Tool", subfolder "Compensation".



6.3.7 Monitored items

An OPC UA client can subscribe to a selection of nodes of interest and let the server monitor these items. Only in case of changes, e.g. to their values, the server notifies the client about such changes. This mechanism reduces the amount of transferred data immensely. Besides the reduction of bandwidth this mechanism introduces further advantages and is the recommended mechanism to “read” information from a UA server.

A client can subscribe to different types of information provided by an OPC UA server. The purpose of a subscription is to group these sources of information, called monitored items, together, forming a piece of information called a notification.

A subscription consists of at least one monitored item, which has to be created within the context of a session and can be transferred to another session. To create a session, a secure channel between the client and the server has to be established.

There are two different types of “changes” a client can subscribe to when adding monitored items to the subscription:

- subscribe to data changes of Variable Values (Value attribute of a Variable)
- subscribe to Events of Objects (EventNotifier attribute of an Object)

Publish interval

Clients define MonitoredItems to subscribe to data and Events. Each MonitoredItem identifies the item to be monitored and the Subscription to use to send Notifications. The item to be monitored may be any Node Attribute.

Notifications are data structures that describe the occurrence of data changes and Events. They are packaged into NotificationMessages for transfer to the Client. The Subscription periodically sends NotificationMessages at a user-specified publishing interval, and the cycle during which these messages are sent is called a publishing cycle." (see OPC UA Part 4 - Services 1.03 Specification.pdf (https://opcfoundation.org/))

Sampling interval

Each MonitoredItem created by the Client is assigned a sampling interval that is either inherited from the publishing interval of the Subscription or that is defined specifically to override that rate. [...] The sampling interval indicates the fastest rate at which the server should sample its underlying source for data changes. (see OPC UA Part 4 - Services 1.03 Specification.pdf (https://opcfoundation.org/))

See also

Technical data (Page 163)

6.4 Alarms

6.4.1 Overview

Any OPC UA client supporting Alarms & Conditions connected to the OPC UA server can subscribe to alarms to get the notifications of alarms.
All OPC UA Clients that have subscribed for SINUMERIK alarms will be provided with an alarm as soon as it becomes active. Also if the alarm becomes inactive, the status of the corresponding alarm/s will be updated automatically.
Alarms and Conditions support subscription of all the pending and active alarms of the SINUMERIK system. Part program messages are not supported as part of Alarms and Conditions, but can be received using data access. The OPC UA Server provides all alarms that will be provided by the SINUMERIK AlarmService:

- HMI alarms
- NCK alarms including drive alarms
- Diagnostic buffer alarms
- PLC alarms (FC10)
- Alarm_S(Q) alarms (SFC17/18, PDiag, HiGraph, S7-Graph) with results of criteria analysis.

Multi language support for the alarms and warnings messages are supported and the required alarm language can be selected during session creation in OPC UA Client. If the desired language is not supported in the operate, the default English language is supported.
The SINUMERIK Alarm object is of the "CNCAlarmType" which is defined in the Companion Specification "OPC UA Information Model for CNC Systems (http://opcfoundation.org/UA/CNC/)".

Part program messages

Part program messages are not considered as alarms from OPC UA point of view.

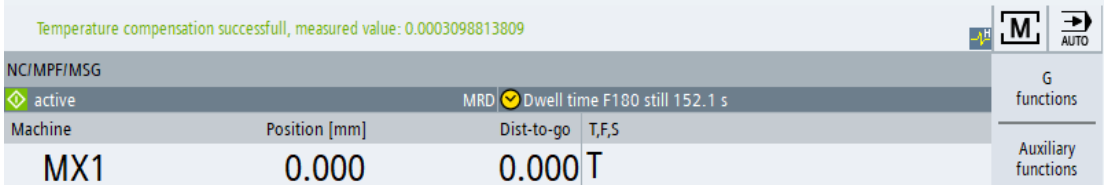


Figure 6-4 Part program messages

They will not be reported in an alarm subscription. In order to have access to part program messages, use the variable path: "/Channel/ProgramInfo/msg".

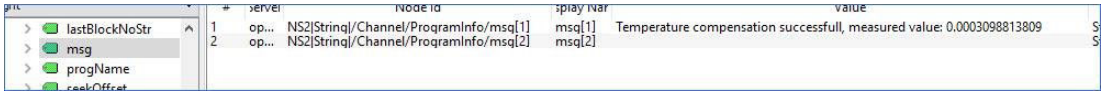


Figure 6-5 Variable path

6.4.2 Subscribe / unsubscribe to alarms

Subscribe to alarms

The SINUMERIK Alarm Event object is connected to the SINUMERIK node. To receive the alarms, an event subscription must be placed at the SINUMERIK node. The following example describes how to receive the alarms using the OPC UA Foundation Client:

1. Open the "Quickstart Alarm Condition Client".

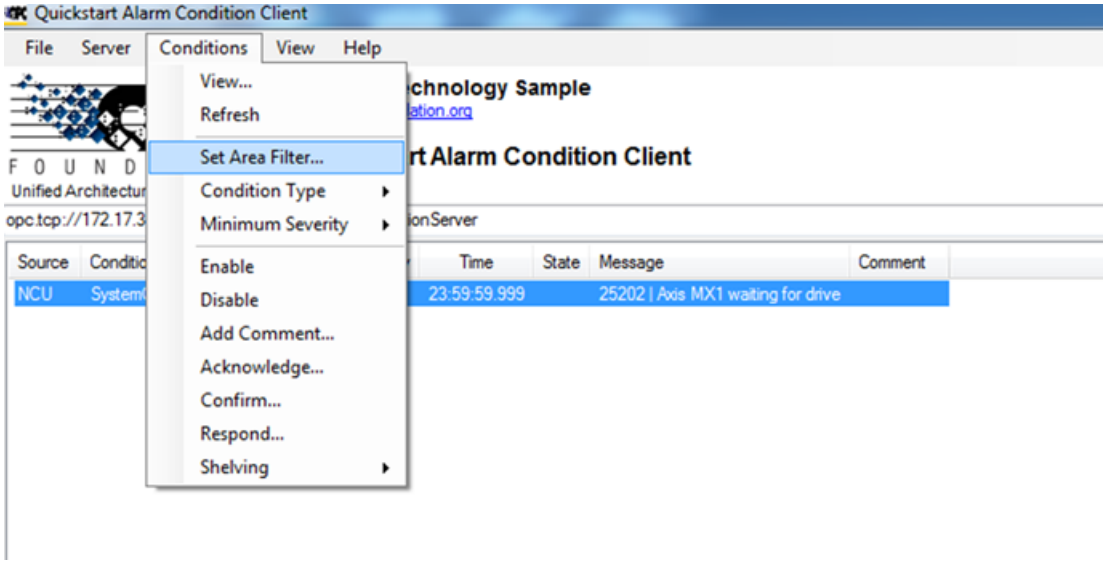


Figure 6-6 Alarm Condition Client

2. Click "Conditions > Set Area Filter...". The "Select Area" window appears.

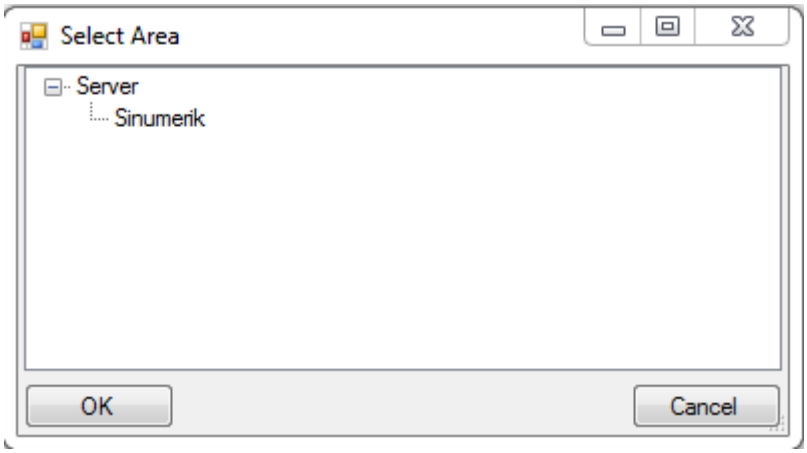


Figure 6-7 The Select Area Window

3. Select "Sinumerik".
4. Click "OK".

The alarms will be displayed on the screen.

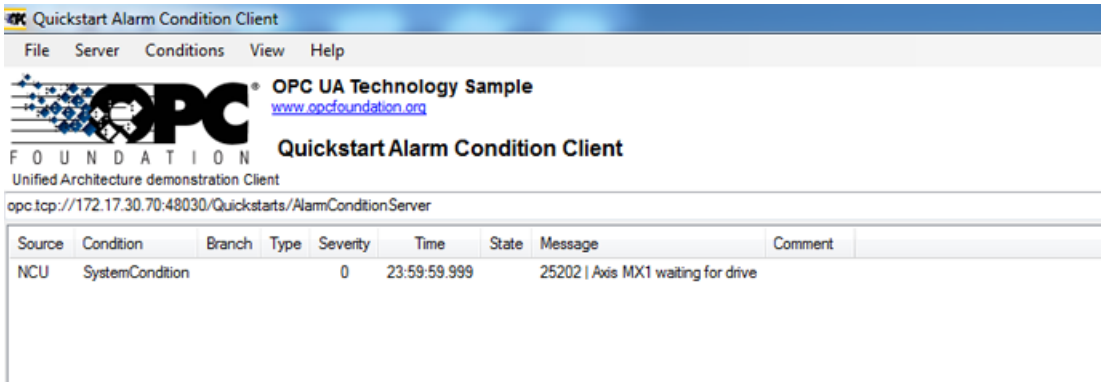


Figure 6-8 Alarm List

Unsubscribe to alarms

1. Click **"**Conditions > Set Area Filter...". The "Select Area" window appears.
2. Right click on "Sinumerik" and select **"**Remove Monitored Item**"** to unsubscribe the server from the Quickstart Alarm Condition Client.

6.4.3 Sequence description of alarms

The OPC UA server automatically sends an object of the "CNCAlarmtype" to the OPC UA client containing the single alarm which has just been triggered.

The OPC UA server automatically resends an object of the "CNCAlarmtype" with the same content as when the corresponding alarm was triggered, except a change in the status.

To get all the active alarms, the client has to subscribe to the Sinumerik node.

6.4.4 SINUMERIK Alarm object

6.4.4.1 Description

Every variable or object in the address space of an OPC UA server is called a node. Every node has a server unique node id, its symbolic name, addressing information inside the address model and some other attributes.

Events are by themselves not visible as nodes in the address space. They can only be received via objects. Not all objects can signal events. Whether an object can signal events is specified at the object by the EventNotifier attribute. Only objects where this attribute has been set can be specified in the Event Monitored Item and received in Clients Events.

The Server Object serves as root notifier, that is, its EventNotifier Attribute shall be set providing Events. However Server object will not be allowed to subscribe for the Events. Only the "Sinumerik" Object node is accessible and can subscribe to the events.

6.4.4.2 OPC UA event messages and alarms

Access to alarms

User access right is required to subscribe the Events of the Sinumerik object. User access right with access permission has to be set to “SinuReadAll” or “AlarmRead”.The access right is provided using Method Call “GiveUserAccess” as shown below.

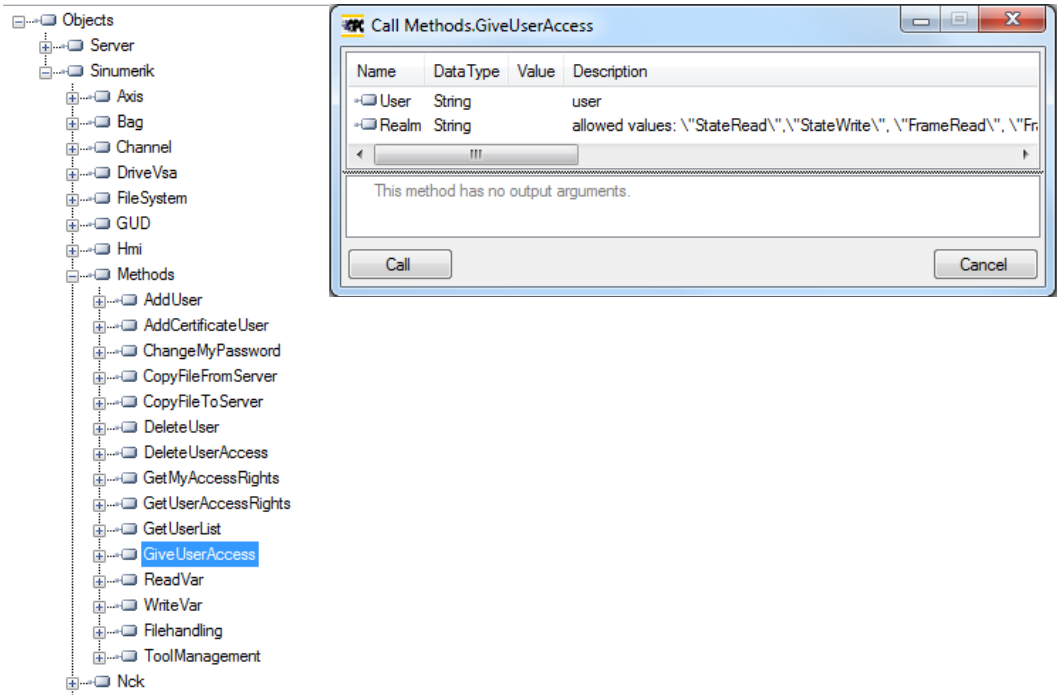


Figure 6-9 Alarm access rights

If the client does not have the access with “SinuReadAll “or “AlarmRead” and user tries to subscribe to the Events, server will return error code with “BadUserAccessDenied”.

Event types

The SINUMERIK Alarm object is of the “CNCAlarmType” which is defined in the Companion Specification “OPC UA Information Model for CNC Systems (http://opcfoundation.org/UA/CNC/)”.

The root of the derivation hierarchy is the BaseEventType. The types for Alarms and Conditions are available below the ConditionType. The Application-specific event types such as CncAlarmType can be derived. The CncAlarmType extends the DiscreteAlarmType.

An alarm is composed of various nested or parallel state machines. Monitoring can generally be enabled or disabled. If monitoring is enabled, the alarm can be active or otherwise inactive. Acknowledgment, confirm and comments of alarms is currently not supported.

The basic type for all condition objects is the condition type. It is derived from BaseEventType. All mechanisms for alarm processing work even without the condition objects are contained in the address space.

If a condition object changes one or several states, the server sends an event with the requested event fields to the client. So only the alarms, where a status change happens after the

connection is established, will be sent. To receive all currently active alarms the refresh method can be used.

CncAlarmType

The CncAlarmType, which is specified in the Companion Specification "OPC UA Information Model for CNC Systems" is derived from the DiscreteAlarmType, which is defined by the OPC Foundation.

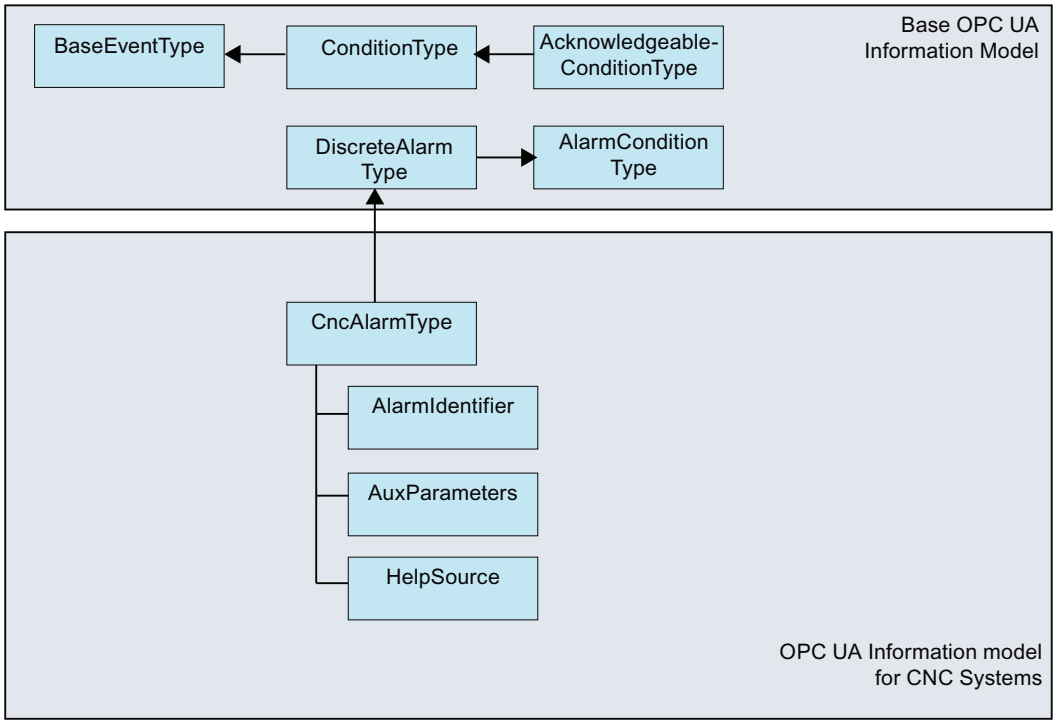


Figure 6-10 OPC UA Information Model for CNC Systems

Description of the CncAlarmType

Since the CncAlarmType is derived from a number of types as you can see in Figure 5-8, it does not only contain the three attributes AlarmIdentifier, AuxParameters and HelpSource, but also all the other attributes which are inherited from the objects.

Attributes of BaseEventType

Attribute	Data type	Mapping with respect to SINUMERIK	M/O	Description
EventId	String	Unique node id generated from SINUMERIK system.	M	EventId is generated by the server to uniquely identify a particular Event Notification. The EventId shall always be returned as value and the server is not allowed to return a StatusCode for the EventId indicating an error.
EventType	NodeId	It is always set to 'CncAlarmType'.	M	The EventType shall always be returned as value and the server is not allowed to return a StatusCode for the EventType indicating an error.
SourceNode	NodeId	Alarm source identifier provided by SINUMERIK system.	M	SourceNode identifies the Node that the Event originated from. If the Event is not specific to a Node, the NodeId is set to null.
SourceName	String	Supported alarm source names are HMI, NCK, and PLC.	M	SourceName provides a description of the source of the Event. This could be the string-part of the DisplayName of the Event source using the default locale of the server. If it is not possible for a CNC system to provide this information in detail, the SourceName should provide the main component responsible for this alarm (e.g. CNC, PLC, or even Channel).
Time	UtcTime	Alarm time stamp	M	Time provides the time of the Event occurred. Once set, intermediate OPC UA servers shall not alter the value.
ReceiveTime	UtcTime	Alarm time stamp of the server.	M	ReceiveTime provides the time the OPC UA server received the Event from the underlying device of another server.
Message	Localized Text	Reading attributes via (SLAE_EV_ATTR_MSG TEXT)	M	Alarm Message provides a human readable and localizable text description of the Event.
Severity	UInt16	Reading attributes via (SLAE_EV_ATTR_SEVE RITY)	M	Severity of the event message. The range of values of the severity is from 1 to 1000, where 1000 corresponds to the highest severity.
LocalTime	TimeZoneDataType	Offset and the DaylightSavingInOffset flag	O	LocalTime is a structure containing the Offset and the DaylightSavingInOffset flag. The Offset specifies the time difference (in minutes) between the Time Property and the time at the location in which the event was issued. If DaylightSavingInOffset is - TRUE: Standard/Daylight savings time (DST) at the originating location is in effect and Offset includes the DST correction. FALSE: The Offset does not include DST correction and DST may or may not have been in effect.

Severity of Alarms

SINUMERIK systems use three severity levels (e.g. Information, Warning and Error). The table below shows the values at SINUMERIK system and its mapping in OPC UA server/client:

Severity Level	SINUMERIK System	OPC UA server/client
Information	0-1	1
Warning	2-999	500
Error	1000	1000

Additional attributes of the ConditionType

Attribute	Data type	Mapping with respect to SINUMERIK	M/O	Description
ConditionClassId	NodeId	Unique node id (sum of alarm id and alarm instance)	M	String NodeID SystemConditionClassType
ConditionClassName	String	Set to "SystemConditionClassType"	M	SystemConditionClassType
ConditionName	String	Set to "SystemCondition".	M	ConditionName identifies the Condition instance that the Event originated from. It can be used together with the SourceName in a user display to distinguish between different Condition instances.
Retain	Boolean	True when the alarm is active. False otherwise.	M	Information whether or not the alarm shall be displayed. This is set to true by default.

Quality	String	According to SINUMERIK quality attribute, below string will be set:
		• BAD
		• GOOD
		• UNCERTAIN
			M	The quality provides information about the reliability of an alarm.
				Possible values of SINUMERIK:
				`AlarmQuality.QUALITY_BAD = 0`
				`AlarmQuality.QUALITY_GOOD = 192`
				`AlarmQuality.QUALITY_UNCERTAIN = 64`

LastSeverity	UInt16	Reading attributes via(SLAE_EV_ATTR_SEVERITY)	M	LastSeverity provides the previous severity of the ConditionBranch. Initially this Variable contains a zero value; it will return a value only after a severity change. The new severity is supplied via the Severity Property which is inherited from the BaseEventType.
BranchId	NodeId	Null	M	BranchId is Null for all Event Notifications that relate to the current state of the Condition instance.
Comment	LocalizedText	Null	M	The value of this Variable is set to null.
ClientUserId	String	Null	M	The value of this Variable is set to null.
Enable		Not supported	M	Servers do not expose Condition instances in the AddressSpace.
Disable		Not supported	M	Servers do not expose Condition instances in the AddressSpace.

Attribute	Data type	Mapping with respect to SINUMERIK	M/O	Description
AddComment		Not supported	M	Not supported and the result code should return Bad_MethodInvalid.
ConditionRefreshMethod			None	When the method is called up, an event with the current state is triggered for the calling client for all conditions. Only those conditions are updated for which the Retain flag has been set.

Additional attributes of the AcknowledgeableConditionType

Attribute	Data type	Mapping with respect to SINUMERIK	M/O	Description
AckedState	Localized text	True / False	M	AckedState when FALSE indicates that the Condition instance requires acknowledgement for the reported Condition state. When the Condition instance is acknowledged, the AckedState is set to TRUE.
ConfirmedState	LocalizedText	True / False	O	ConfirmedState indicates whether it requires confirmation.
EnabledState	Localized text	True / False	M	Always set to true
Acknowledge		Not supported	M	Not Supported and the return error code shall be Bad_MethodInvalid.
Confirm			O	The Confirm Method is used to confirm an Event Notifications for a Condition instance state where ConfirmedState is FALSE. Normally, the NodeId of the object instance as the ObjectId is passed to the Call Service. However, some Servers do not expose Condition instances in the AddressSpace. Therefore all Servers shall also allow Clients to call the Confirm Method by specifying ConditionId as the ObjectId. The Method cannot be called with an ObjectId of the AcknowledgeableConditionType Node.

Additional attributes of the CncAlarmType

The CNCAlarmType is defined in the VDW Companion Specification “OPC UA Information Model for CNC Systems”.

Attribute	Data type	Mapping with respect to SINUMERIK	M/O	Description
AlarmIdentifier	String	Unique Alarm id.	M	Unique alarm number. This mapped to Alarm ID.
AuxParameters	String	All available (out of 10) parameters will be displayed in '' separated value.	M	10 Auxilliary parameter values provided by SINUMERIK system.

6.4.5 Language of alarms

6.4.5.1 OPC UA language specification

The OPC UA server has a built-in data type "LocalizedText" to store the language specific alarm text. This data type defines a structure containing a string in a locale-specific translation specified in the identifier for the locale. The elements are defined in the table below :-

Name	Type	Description
LocalizedText	structure	
text	String	The localized text.
locale	LocaleId	The identifier for the locale (e.g. “en-US”).

The "LocaleId" is a simple data type that is specified as a string that is composed of a language component and a country/region component as specified by IEEE 754-1985 (http://standards.ieee.org/findstds/interps/index.html), IEEE Standard for Binary Floating-Point Arithmetic. The <country/region> component is always preceded by a hyphen.

The format of the LocaleId string is shown below:

<language>[-<country/region>]

- <language> is the two letter ISO 639 code for a language
- <country/region> is the two letter ISO 3166 code for the country/region

You can find **further information** in the specification **OPC UA Part3 - Address Space Model 1.03 Specification.pdf**

6.4.5.2 SINUMERIK language specification

The SINUMERIK system currently supports 31 languages which are mentioned below. These languages are identified by the 3-letter abbreviation that follows Microsoft conventions.

Note

In the list of languages that are mentioned, not every language is supported always.

6.4.5.3 Mapping of SINUMERIK LanguageID with OPC UA LocaleID

Mapping of the SINUMERIK LanguageID with the OPC UA specific LocaleId for each of the supported languages.

Language	SINUMERIK LanguageID	OPC UA Specific LocaleId
German - Germany	deu	de-DE
English - United Kingdom	eng	en-GB
Chinese (Simplified)	chs	zh-CHS
Chinese (Traditional)	cht	zh-CHT
Czech - Czech Republic	csy	cs-CZ

Language	SINUMERIK LanguageID	OPC UA Specific LocaleId
Danish – Denmark	dan	da-DK
Bulgarian - Bulgaria	bgr	bg-BG
Greek – Greece	ell	el-GR
Spanish – Spain	esp	es-ES
Finnish – Finland	fin	fi-FI
French – France	fra	fr-FR
Hindi – India	hin	hi-IN
Croatian – Croatia	hrv	hr-HR
Hungarian – Hungary	hun	hu-HU
Indonesian – Indonesia	ind	id-ID
Italian – Italy	ita	it-IT
Japanese - Japan	jpn	ja-JP
Korean – Korea	kor	ko-KR
Malay – Malaysia	msl	ms-MY
Dutch - The Netherlands	nld	nl-NL
Polish – Poland	plk	pl-PL
Portuguese - Brazil	ptb	pt-BR
Romanian - Romania	rom	ro-RO
Russian – Russia	rus	ru-RU
Slovak – Slovakia	sky	sk-SK
Slovenian – Slovenia	slv	sl-SI
Swedish – Sweden	sve	sv-SE
Tamil – India	tam	ta-IN
Thai – Thailand	tha	th-TH
Turkish – Turkey	trk	tr-TR
Vietnamese - Vietnam	vit	vi-VN

In the above list “OPC UA Specific LocaleId” is used by the OPCU UA client to connect with the server.

6.4.6 OPC UA alarms and conditions constraints

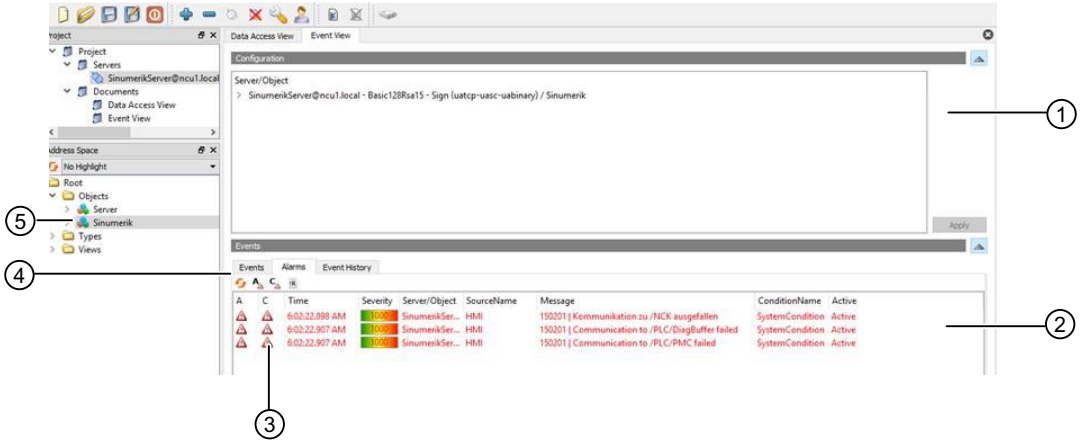
Below are the features which are not supported in this version:

- Acknowledgements and confirmation of the alarms.
- Part program messages
- Only alarm text will be available in localized text. All other attributes will be available in English only.

6.4.7 OPC UA alarms and conditions client

User interface

The figure and table below describes the user interface of the UaExpert client example with which the information of the namespace of an OPC UA server can be conveniently accessed.



① The Alarm window

② Displays the received events with preconfigured event fields. The standard event fields are:

- In the Events tab: Time, ReceiveTime, Severity, SourceName, Message, EventType and SourceNode
- In the Alarms tab: AcknowledgeState, Time, Severity, SourceName, Message, ConditionName, ActiveState and Retain Flag

③ In the first column of the Alarm tab, a symbol indicates whether an event has already been Acknowledged. (red flag: unacknowledged, green checkmark: acknowledged)

④ The Alarm / Event Subscription View

⑤ Alarm / Event Instances:

The user needs to subscribe to these instances (by dragging or by configuring).

Figure 6-11 User interface UaExpert client

6.4.8 OPC UA multi-language alarms and conditions client

The OPC UA client must explicitly provide the OPC UA specific language "LocaleId" to change the alarm texts. Below is an example of changing the client language using OPC UA foundation stack client.

```
//Create and connect session
var preferredLocalesList = new List<String>();
preferredLocalesList.Insert(0, "de-DE");

Session  mSession = Session.Create(
    ApplicationConfig,
    mEndpoint,
    true,
    "MySession",
    60000,
    UserIdentity,
    preferredLocalesList //preferred locale list
    );
```

Figure 6-12 OPC UA multi-language alarms and conditions client using OpcUa foundation .Net Client

In the case of UaExpert client proceed as follows:

1. Open the “Configure UaExpert” window under "Settings" Tab in the client
2. Provide the OPC UA specific "LocaleId" as value for the parameter "General.LocaleId".
3. Then connect to the server.

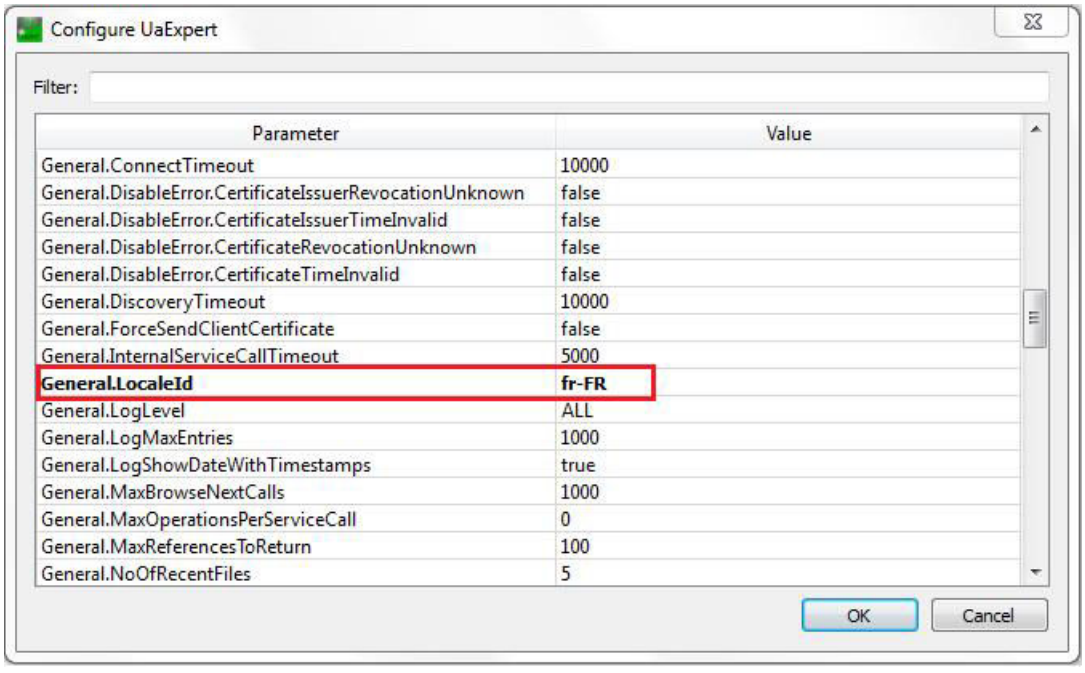


Figure 6-13 Client User Interface for changing Session Language

Language	OPC UA Specific LocaleId
German - Germany	de-DE
English - United Kingdom	en-GB
Chinese (Simplified)	zh-CHS
Chinese (Traditional)	zh-CHT
Czech - Czech Republic	cs-CZ
Danish – Denmark	da-DK
Bulgarian - Bulgaria	bg-BG
Greek – Greece	el-GR
Spanish – Spain	es-ES
Finnish – Finland	fi-FI
French – France	fr-FR
Hindi – India	hi-IN
Croatian – Croatia	hr-HR
Hungarian – Hungary	hu-HU
Indonesian – Indonesia	id-ID
Italian – Italy	it-IT
Japanese - Japan	ja-JP
Korean – Korea	ko-KR
Malay – Malaysia	ms-MY
Dutch - The Netherlands	nl-NL
Polish – Poland	pl-PL
Portuguese - Brazil	pt-BR
Romanian - Romania	ro-RO
Russian – Russia	ru-RU
Slovak – Slovakia	sk-SK
Slovenian – Slovenia	sl-SI
Swedish – Sweden	sv-SE
Tamil – India	ta-IN
Thai – Thailand	th-TH
Turkish – Turkey	tr-TR
Vietnamese - Vietnam	vi-VN

6.5 File system

6.5.1 Overview

SINUMERIK OPC UA supports the standard OPC UA file and folder objects, which allows transfer of files as well as the manipulation of the file systems.

Furthermore, the server offers 2 comfort methods to copy NC part programs from the OPC UA client to the OPC UA server and vice versa. Due to the nature of the method this comfort methods are limited to a file size of 16 MB. For bigger files please use the file and folder objects as described in chapter File transfer exceeding 16 MB between client and server (Page 122).

Operations

This allows an OPC UA client to use the following operations within the part of the SINUMERIK file system:

1. Create files/directories
2. Copy files/directories
3. Moving files/directories
4. Deleting files/directories
5. Renaming files/directories

File system

The standard OPC UA file system is placed in the SINUMERIK folder and the file structure of the NCU is as shown below:

1. Part Programs
2. Sub Programs
3. Work Pieces
4. NCExtend (External SD Card/internal SD Card)

   Note

   For 840D sl

   For NCU, external SD Card/internal SD Card is supported.

   For IPC/PCU, SSD/Harddisk is supported.

5. ExtendedDrives (USB/Networkshare)

   Note

   The ExtendedDrives folder will only be displayed if there are external drives available. Please keep in mind that a licence my be required to use these external drive.

Note

NCExtend and ExternalDrives option is supported for SINUMERIK Operate version 4.7 or later.

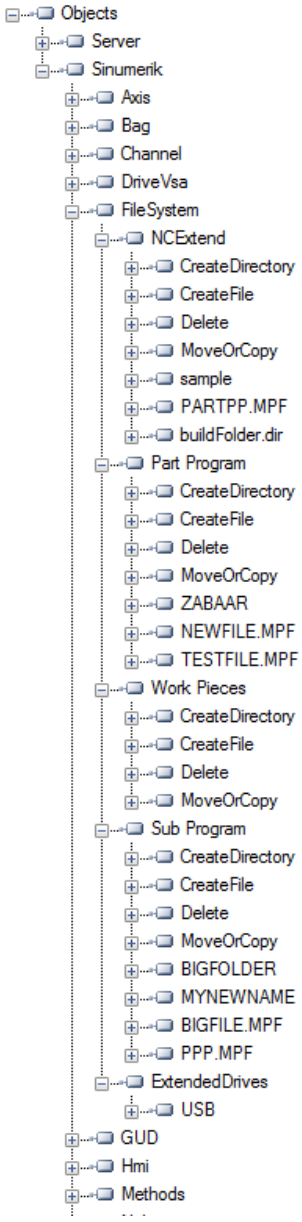


Figure 6-14 The file system

6.5.2 Prerequisites

The OPC UA server allows the OPC UA client to support the transfer of files between the client and the server.

As a user, you will require user access rights to access these files from the server. The access rights are provided using the "GiveUserAccess" method. The following access rights can be provided for the file system (also see chapter List of rights (Page 86)):

- FsRead for the standard file system methods like Open, GetPosition, Read as well as the CopyFileFromServer method.
- FsWrite for the standard file system methods like CreateDirecotry, CreateFile, Delete, MoveOrCopy, Write, SetPosition, Close as well as the CopyFileToServer method.

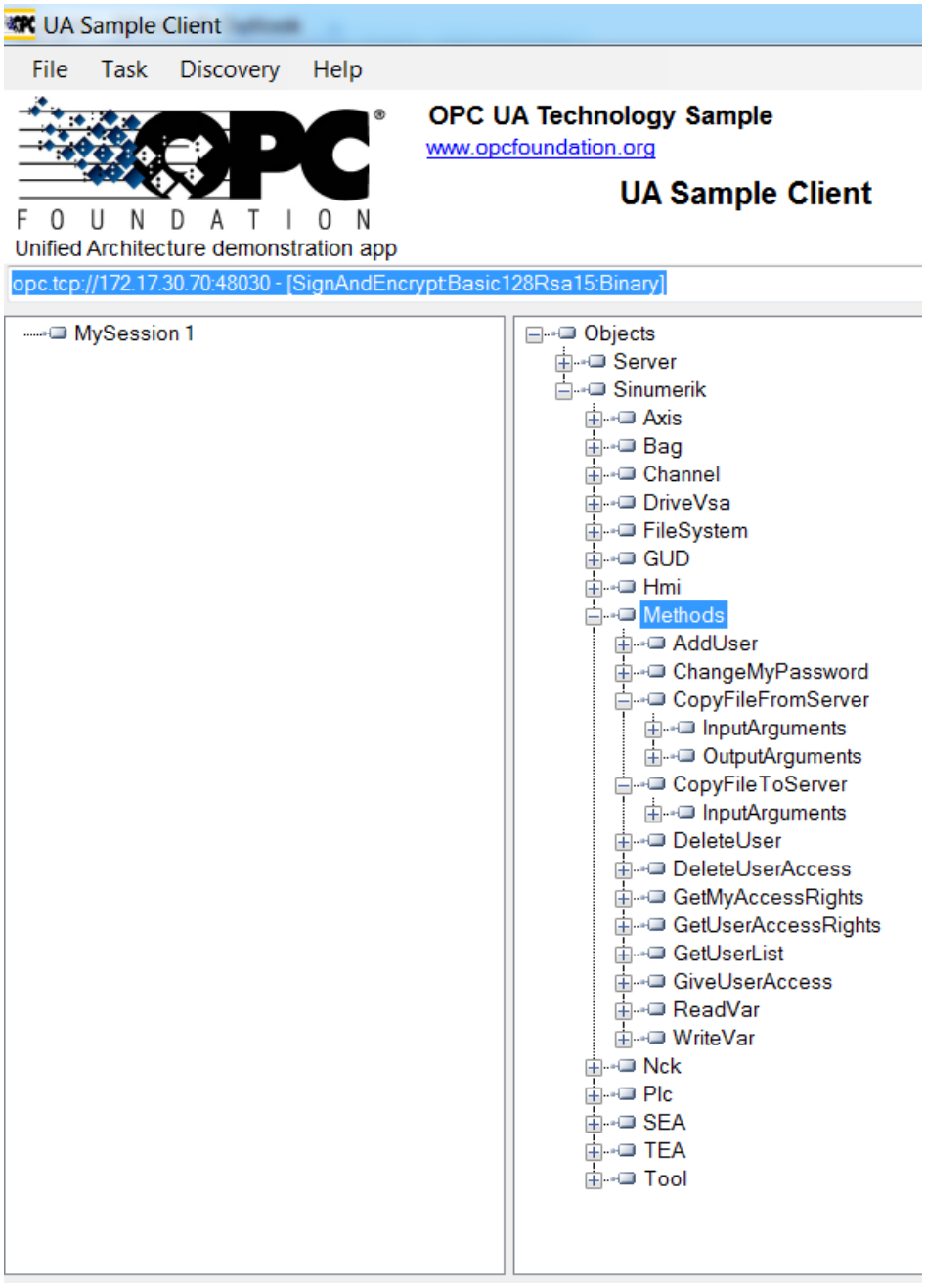


Figure 6-15 Standard Method

6.5.3 Standard file system support

6.5.3.1 File transfer with standard methods

The SINUMERIK OPC UA server supports the "FileType"/"FolderType" as described in the OPC UA Specification Part 5, which allows manipulating files and folders via OPC UA.

Folder methods

The folders, "Part Programs", "Sub Programs", "Work Pieces", "NCExtend", and "ExtendedDrives" are of the "FolderType", which contain the following methods:

Method/Attribute	Description
CreateDirectory	To create new folders under parent folder.
CreateFile	To create new file under parent folder.
Delete	To delete folder and file under parent folder.
MoveOrCopy	To copy or move files from source to destination within server filesystem.

You can create, delete, move or copy folders and files using the above methods. When you create a new folder using "CreateDirectory"', a new node will be created with "FolderType" and name provided by the user in OPC UA client. This folder contains all methods and attributes specified in above table.

The node in the address space, under which the "CreateDirectory" method is called, is the "parent" node of the new folder node.

The folder methods exist under all folder type objects in the file system. Please note that you must always call the method under the direct parent node of the file or folder.

For the methods "Delete" and "MoveOrCopy" you must always provide the full identifier of the node to be moved, copied or deleted.

Whenever you create a new file using the method "CreateFile", a new node will be created with "FileType" with a user provided name. This file again contains all methods and attributes specified in the table above. The node in address space, under which the "CreateFile" method is called, is the "parent" node of the new file node. For specific information for the described methods, check the Typedefinition in the OPC UA Specification Part 5.

Examples for the usage of the folder methods

Name	Signature	Usage
CreateDirectory	[in] String directoryName [out] NodeId directoryNodeId	Call from parent folder/directory, e. g.: Sinumerik/FileSystem/Work Pieces
CreateFile	[in] String fileName [in] Boolean requestFileOpen [out] NodeId fileNodeId [out] UInt32 fileHandle	Call from parent folder/directory, e. g.: Sinumerik/FileSystem/Part Program File-name including extension, e. g.: myPart-Prog.mpf

Name	Signature	Usage
Delete	[in] NodeId objectToDelete	Call from parent folder/directory, e. g.: Sinumerik/FileSystem/Part Program
MoveOrCopy	[in] NodeId objectToMoveOrCopy [in] NodeId targetDirectory [in] Boolean createCopy [in] String newName [out] NodeId newNodeId	Call from parent folder/directory of object to move/copy, e. g.: copy a part program the parent folder is: Sinumerik/FileSystem/Part Program

Note

For further details on methods and method signatures please refer to OPC UA Specification Part 5.

File methods

All files which are in the above mentioned folders will be of the "FileType" type and consist of the following methods and properties:

Method/Attribute	Description
Open	Opens the file either in read/write mode.
Read	Reads contents of the file.
Write	Writes data to the file. (if write permission is available)
Close	Closes the file. (succeeds if file is open)
GetPosition	Gets the position of current position of file pointer while file read/write operation.
SetPosition	Sets the position of current position of file pointer while file read/write operation.
OpenCount	Gives the number of file open instances.
Size	Gives the file size details.
UserWritable	Set to true if current user has access to modify the content of the file.
Writable	Set to false if the file is read only.

Whenever you create a new file using the method "CreateFile", a new node will be created with "FileType" type with a user provided name. This file again contains all methods and attributes specified in the table above. The node in address space, under which the "CreateFile" method is called, is the "parent" node of the new file node. For specific information for the described methods, check the type definition in the OPC UA Specification Part 5 Annex C.

Note

No multiple extensions supported

The methods "CreateFile","CopyFileToServer", "CopyFileFromServer" and "MoveOrCopy" will not support files with multiple extensions (i.e. test.mpf.mpf).

6.5.3.2 File transfer exceeding 16 MB between client and server

For file transfer, the OPC UA specification v1.0X, Part 5, Annex C offers the use of file and folder object methods.

How can a file transfer be implemented in a client using the file and folder object methods?

The basic idea is to open a file and copy the content from location A to B and then close the file.

Therefore to copy a file from the SINUMERIK to an OPC UA client the client needs to do the following:

- Open the file on the SINUMERIK via the Open method,
- then pass the received handle to the Read method and operate on arrays of bytes,
- then close the file via the Close method.

For the other direction, the file has to be created on the SINUMERIK file system first, using the Create method.

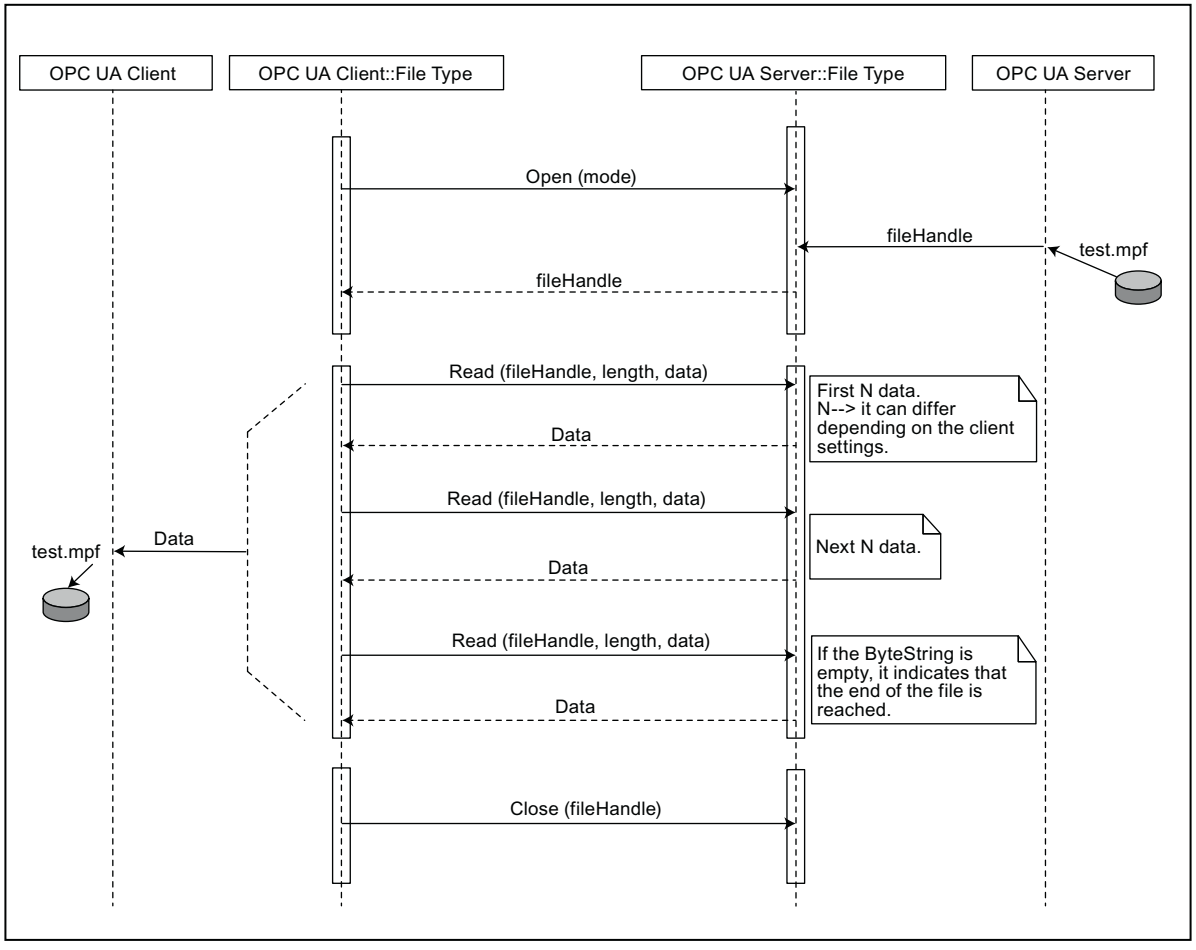


Figure 6-16 File transfer from server to client using standard file system methods

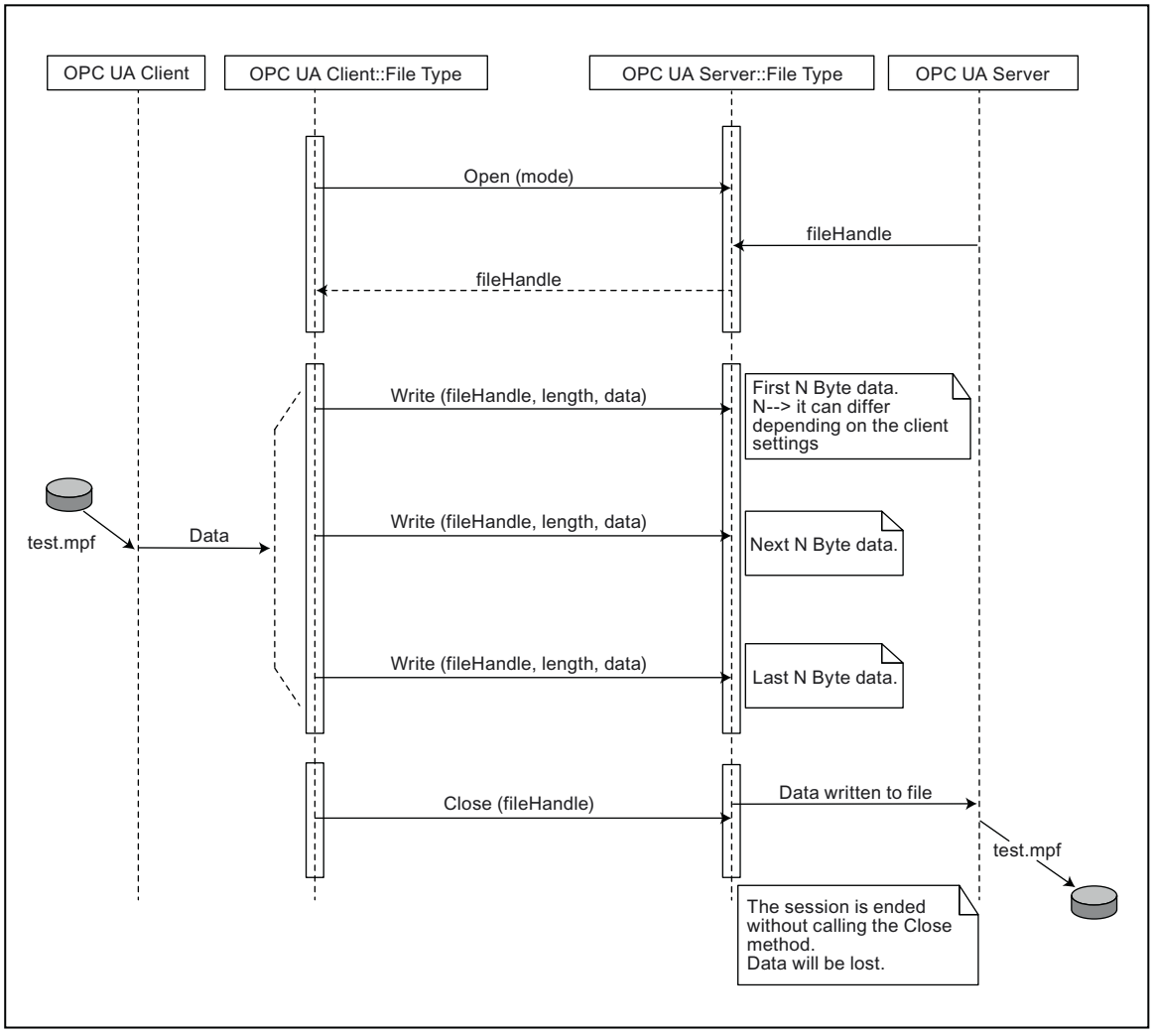


Figure 6-17 File transfer to server from client using standard file system methods

6.5.3.3 Comfort methods for file transfer < 16 MB

In addition to the standard file system, two additional methods are provided to transfer files from server to client and vice versa.

Note

With these methods, you will be able to transfer maximum of 16 MB by default, depending on the client settings. As the maximum ByteString and message size depends on the server and client-side stack limit. For file transfer more than 16 MB, it is recommended to use OPC UA standard file transfer methods.

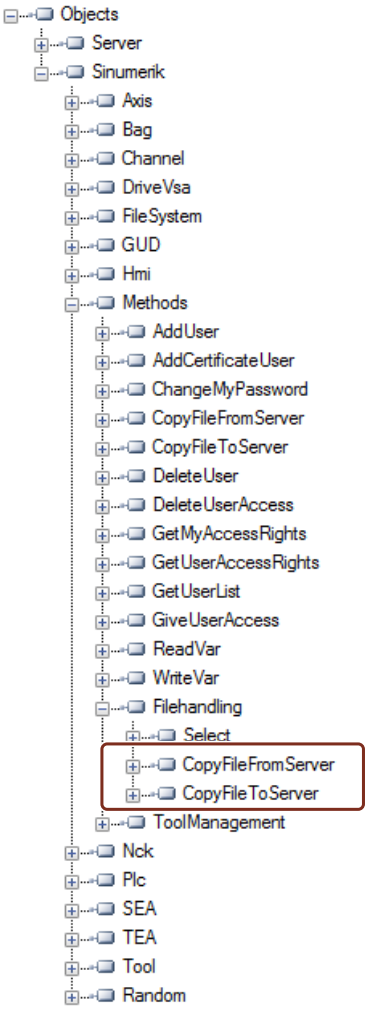


Figure 6-18 Methods for the file transfer

Procedure and Example

1. CopyFileFromServer:
   - Allows copying file from SINUMERIK OPC UA server to client location.
   - The user shall provide the name of the file with full path to be copied.
   - On completion of the file transfer, an appropriate message will be displayed.

Type	Data type	Argument	Description
Input parameter	string	SourceFile	Name of the file need to be copied with absolute path.
Output parameter	ByteString	Data	Raw file data

2. CopyFileToServer:
   - Allows copying a client file to a specified SINUMERIK NC memory location.
   - The user shall select the file to be transferred and specify the location on server.

Type	Data type	Argument	Description
Input parameter	string	TargetFilename	Target file name with absolute path
Input parameter	ByteString	Data	Raw file Data
Input parameter	Boolean Overwrite	Overwrite	True: Overwrite the file if already exists. False: File will not be overwritten.

For example:

The complete path of the files can be provided as below:

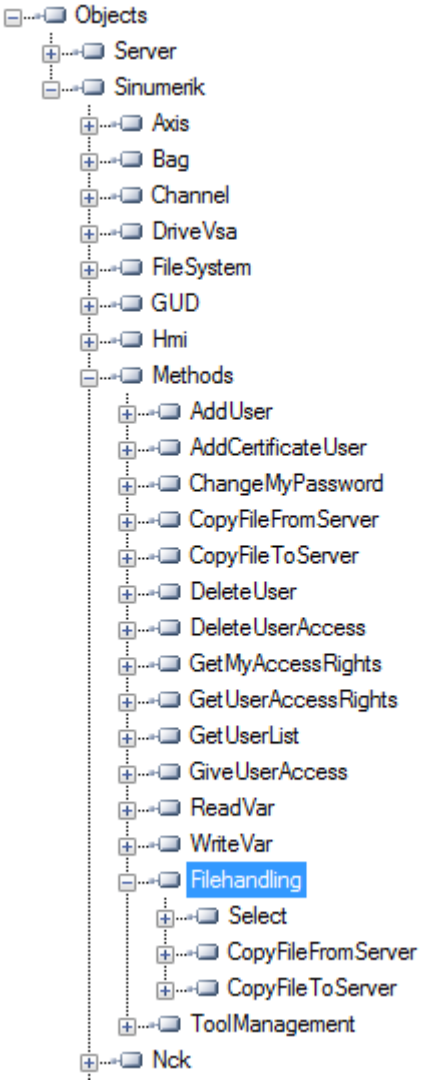
- Sinumerik/FileSystem/Part Program/partprg.mpf
- Sinumerik/FileSystem/Sub Program/subprg.spf
- Sinumerik/FileSystem/Work Pieces/wrkprg.wpf
- Sinumerik/FileSystem/NCExtend/Program.mpf
- Sinumerik/FileSystem/ExtendedDrives/USBdrive/Q3.mpf

6.6 Select

6.6.1 Overview

The "Select" method is provided under "Methods > Filehandling" in the address space, which allows the selecting of a part program from the NC file system. You can call this method and select the file to be executed by providing the node identifier of the file in address space and the channel number.

By calling this method, you can only select the program for execution and not start the execution of the program itself.



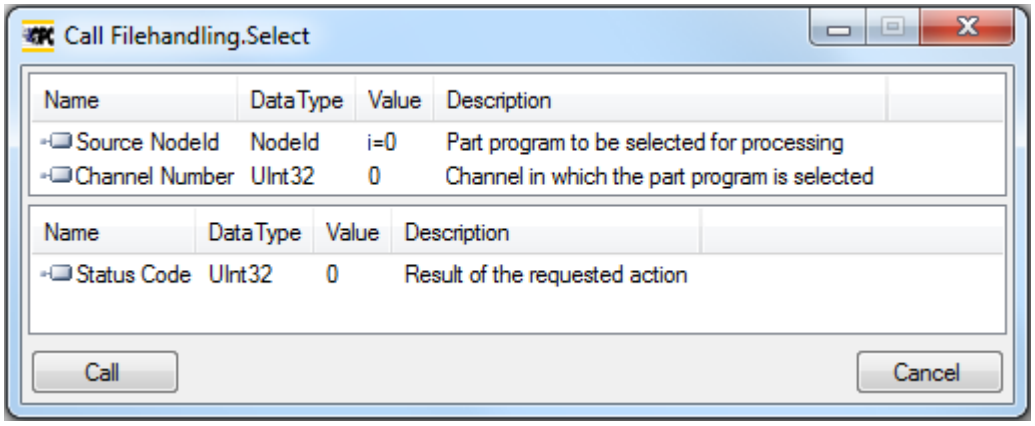
6.6.2 Description

You are allowed to select the part program file for execution from the NC file system and external memory, which includes "local drive", "USB" and "network share". As part of the file system feature, the NC file system is exposed in the OPC UA address space.

There are two input values to be provided to call the "Select" method.

- Node identifier of the file to be selected for execution.
- Channel number.

Each part program file on the file system is associated with a node identifier in the OPC UA address space and is provided as the input. Only one part program can be selected for a channel. An error will be displayed otherwise.



Status code is an output parameter which indicates the error code in case of failures.

6.6.3 Input and output arguments

Signature of the method "Select" is as follows:

```
Select (
[in] string SourceFileNodeId,
[in] int32 ChannelNumber,
[out] int32 Status Code)
```

Argument	Description
SourceFileNodeId	Represents the node identifier of the file with absolute path (which is selected for execution).
Channel Number	A number which represents the channel to be used while program execution.

Prerequisites

- Channel to be used during program execution must be in the state "Reset".
- User with "**ApWrite**" access right can call "Select" method. If the user does not have the access "**ApWrite**" and tries to call "Select" method, it fails and server will return with OpcUa status "**BadUserAccessDenied**".

Note

The access right for the user is provided using the "GiveUserAccess" method.

Status Code of the method call

The following table gives details on values and description on the status of the "Select" method call. As part of output argument, the result code (value) is displayed in the OPC UA client.

Status Code (value)	Description
0	Successful
1	Channel does not exist
2	Part Program cannot be found
3	Channel is not in Reset
4	Target rejected requested action.

Note

No file restriction

Notice that a file with any extension is allowed to be selected through OPC UA "Select" method. OPC UA does not restrict selecting files with any file extension.

Joblists cannot be selected.

OPC UA Status

The following table gives details on values and description of the OPC UA method call status:

Result	Description
Succeeded	Method is executed with success/failure.
OpcUa_BadInvalidArgument	Invalid inputs are provided.
OpcUa_BadUserAccessDenied	User does not have permission to invoke the method.

6.6.4 Example call

Procedure

1. Look for the NodeID of the particular part program you want to select (for example "NC_PROG1.MPF").
2. Navigate in the "File System" node until you reach the particular file.

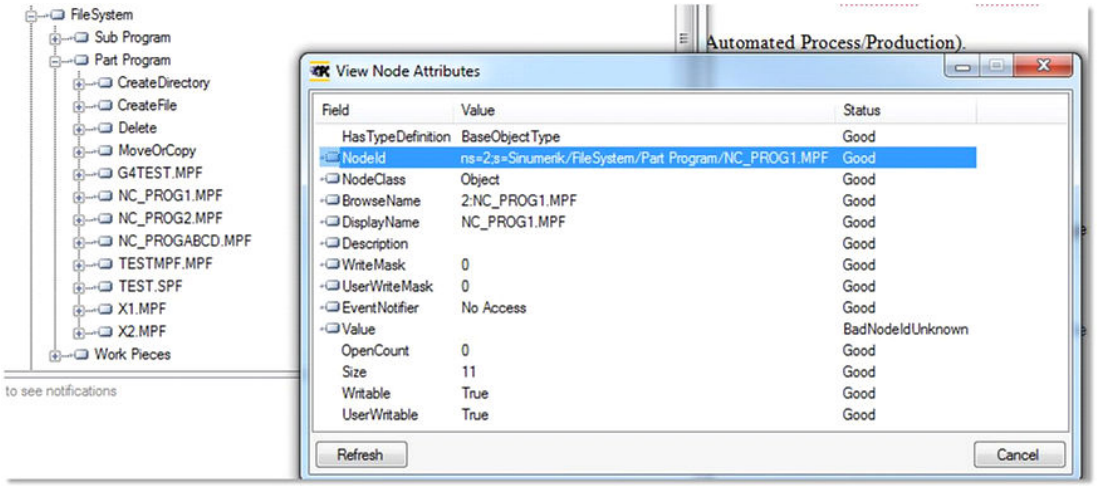


Figure 6-19 Finding of NodeID

3. Specify the NodeID and the channel number in the call of the method.

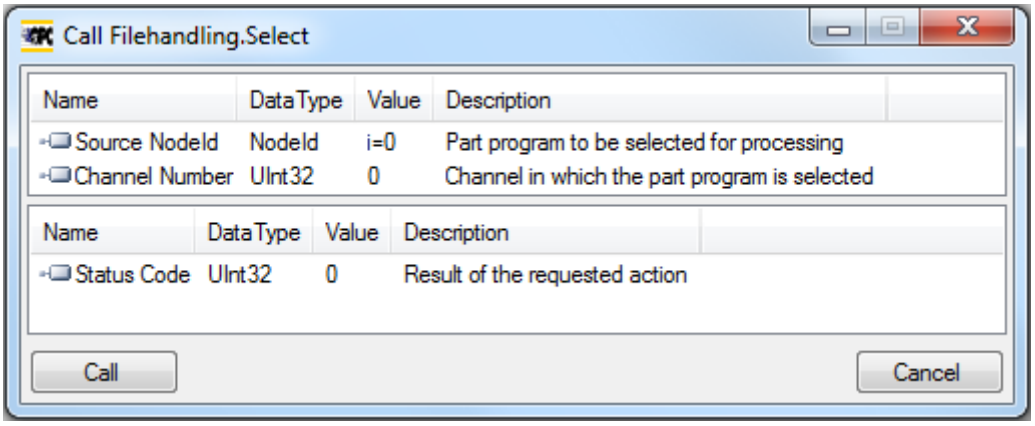


Figure 6-20 Arguments of select method

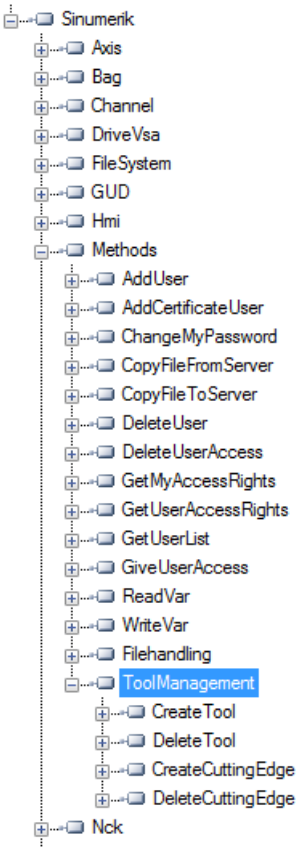
The particular part program will be selected.

6.7 Tool management

6.7.1 Description

The OPC UA server supports the creation and deletion of tools and cutting edges. The methods for this operation can be found under "Sinumerik > Methods > ToolManagement" folder. Following are the four methods present in "ToolManagement" folder:

- CreateTool
- DeleteTool
- CreateCuttingEdge
- DeleteCuttingEdge



Example calls

For example calls of the provided methods, please refer to the shown screenshots of OpcFoundation Client.

Prerequisites

User with "ToolWrite" access right can call "ToolManagement" methods. If the user does not have the access "ToolWrite" and tries to call "ToolManagement" methods, it fails and server will return with OpcUa status "**BadUserAccessDenied**".

Note

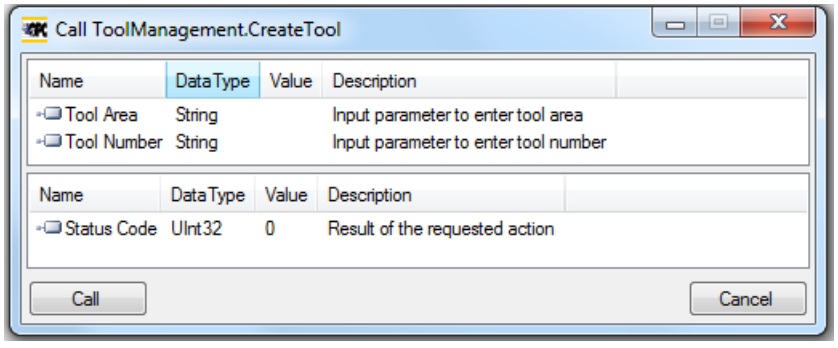
The access right for the user is provided using the "GiveUserAccess" method.

6.7.2 CreateTool

The "CreateTool" method is used to create a new tool with a special T-number in Tool List section of the SINUMERIK, and appears under the folder "Methods/ToolManagement". The CreateTool method does not contain the settings of tool parameters. The tool parameters e.g.: tool type, cutting edge date etc. are set via data access functions.

The CreateTool method has two input parameters and one output parameter.

```
Signature:
CreateTool(
[in] string ToolArea
[in] string ToolNumber
[out] Uint32 StatusCode
)
```



The following table will give details about the parameters of the method:

Type	Parameters	Description
Input	Tool Area	Input parameter to enter tool area.
Input	Tool Number	5 digit number given to the created tool. For range of number please refer to 828D or 840D sl documentation respectively.
Output	Status Code	A number which gives a feedback if the method was executed successfully or not.

The method returns a value which indicates whether the creation was successful or not. If the creation was not successful the return value will give information about the reason of the failure.

Status code

The status code is the result of the requested action which is a number as shown in the table below:

Status Code	Reason
0	OK.
1	Tool area does not exist.
2	Tool number out of range.(Reason wrong parameter)
3	Tool number exists already.
4	Maximum number of tools reached.

Method Result Codes

Result	Description
Succeeded	Method executed with success/failure reason.
BadInvalidArgument	Arguments provided are not correct.
BadUserAccessDenied	"ToolWrite" access is not provided.

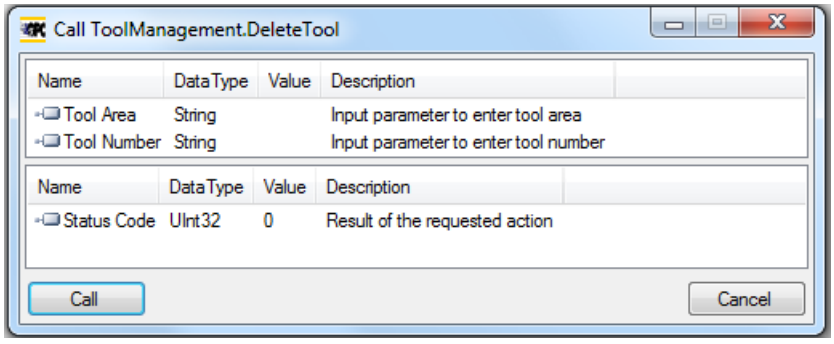
6.7.3 DeleteTool

The "DeleteTool" method is used to delete an existing tool in Tool List section of the SINUMERIK, and appears under the folder “Methods/ToolManagement”.

The method deletes the tool with all cutting edges in all data blocks where it is saved.

```
DeleteTool(
[in] string ToolArea
[in] string ToolNumber
```

```
[out] Uint32 StatusCode
)
```



The following table will give details about the Parameters of the method:

Type	Parameters	Description
Input	Tool Area	Input parameter for the end user to enter tool area.
Input	ToolNumber	5 digit number which is to be deleted. For range of number please refer to 828D or 840D sl documentation respectively.
Output	StatusCode	A number which gives a feedback if the method was executed successfully or not.

The method returns a value which indicates whether the delete was successful or not. If the delete was not successful the return value will give information about the reason of the failure.

Status code

If the deletion of the tool was not successful the return value will give information about the reason of the failure which are explained in the table below.

StatusCode	Description
0	OK.
1	Tool area does not exist.
2	Tool number out of range.(Reason wrong parameter)
3	Tool does not exist.
6	Tool active.(Reason tool in use)

Method Result Codes

The Result return "Succeeded" when the method is correctly executed and the *StatusCode* gives the reason of Success/Failure.

It returns "BadInvalidArgument", if inputs are not according to OPC UA standards.

Result	Description
Succeeded	Method executed with success/failure reason.
BadInvalidArgument	Arguments provided are not correct.
BadUserAccessDenied	"ToolWrite" access is not provided.

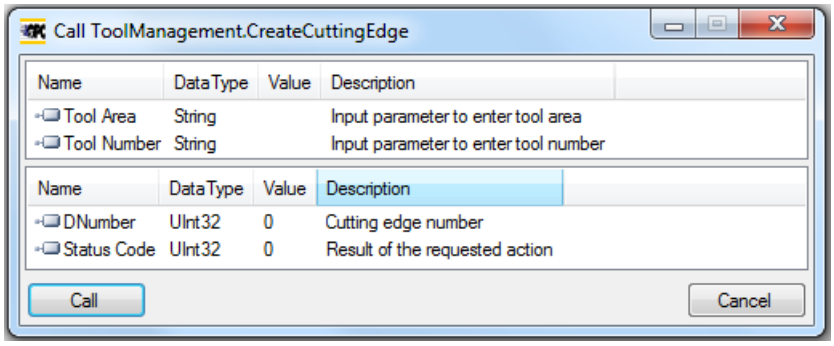
6.7.4 CreateCuttingEdge

The "CreateCutting Edge" method is used to create a new cutting edge of an existing tool in “Tool List” section of the SINUMERIK. The next superior free D number will be created.

The ”CreateCuttingEdge” method appears under the folder “Methods/ToolManagement”. This method does not contain the settings of cutting edge parameters.

The CreateCuttingEdge method has two inputs and two output parameters.

```
Signature:
CreateCuttingEdge(
[in] string ToolArea
[in] string ToolNumber
[out] Uint32 DNumber
[out] Uint32 StatusCode
)
```



The following table will give details about the parameters of the method:

Type	Parameters	Description
Input	Tool Area	Input parameter to enter tool area.
Input	Tool Number	5 digit number which is to be deleted. For range of number please refer to 828D or 840D sl documentation respectively.

Type	Parameters	Description
Output	DNumber	Cutting Edge Number of the tool.
Output	Status Code	A number which gives a feedback if the method was executed successfully or not.

The method returns a value which indicates whether the creation was successful or not. If the creation was successful the DNumber under which the new cutting edge was created will be returned. If the creation was not successful the return value will give information about the reason of the failure.

Status code

The status code is the result of the requested action and is represented by a number, as shown in the table below:

Status Code	Reason
0	OK.
2	Tool number out of range.
4	Maximum cutting edges reached no more cutting edges.
5	There is no tool for which edge can be created. (Reason wrong tool area or tool number)

Method Result Codes

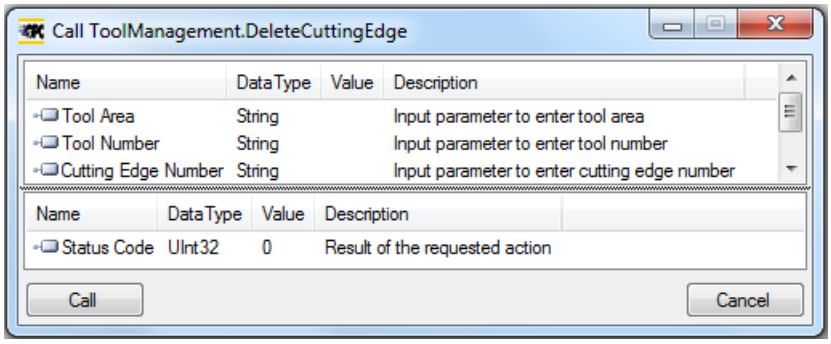
Result	Description
Succeeded	Method executed with success/failure reason.
BadInvalidArgument	Arguments provided are not correct.
BadUserAccessDenied	"ToolWrite" access is not provided.

6.7.5 DeleteCuttingEdge

The "DeleteCuttingEdge" is used to delete a cutting edge of an existing tool in "Tool List" section of the SINUMERIK. This method appears under the folder "Methods/ToolManagement".

The DeleteCuttingEdge method has three input and one output parameters.

```
Signature:
DeleteCuttingEdge(
[in] string ToolArea
[in] string ToolNumber
[in] string CuttingEdgeNumber
[out] Uint32 StatusCode
)
```



Following table will give details about the Parameters of the method:

Type	Parameters	Description
Input	Tool Area	Input parameter to enter tool area.
Input	Tool Number	Tool number of an existing tool whose cutting edge is to be deleted.
Input	Cutting Edge Number	5 digit number which is to be deleted. For range of number please refer to 828D or 840D sl documentation respectively.
Output	Status Code	A number which gives a feedback if the method was executed successfully or not.

The method should return a value which indicates whether the delete was successful or not. If the delete was not successful the return value should give information about the reason of the failure.

Status code

The status code is the result of the requested action which is a number as shown in the table below:

Status Code	Reason
0	OK
2	Tool number out of range.
4	Cutting edge does not exist.
5	There is no tool for which edge can be deleted (Reason wrong tool area or tool number)
6	Tool active. (Reason tool in use)
7	The first cutting edge cannot be deleted.

Method Result Codes

Result	Description
Succeeded	Method executed with success/failure reason.
BadInvalidArgument	Arguments provided are not correct.
BadUserAccessDenied	"ToolWrite" access is not provided.

Diagnosis

7

7.1 Overview

Overview

The OPC UA server offers a variety of diagnostics information, as described in the OPC UA Standard Part 5 - "Information Model", Chapter 6.

This diagnostics information can be found under the Server Node:

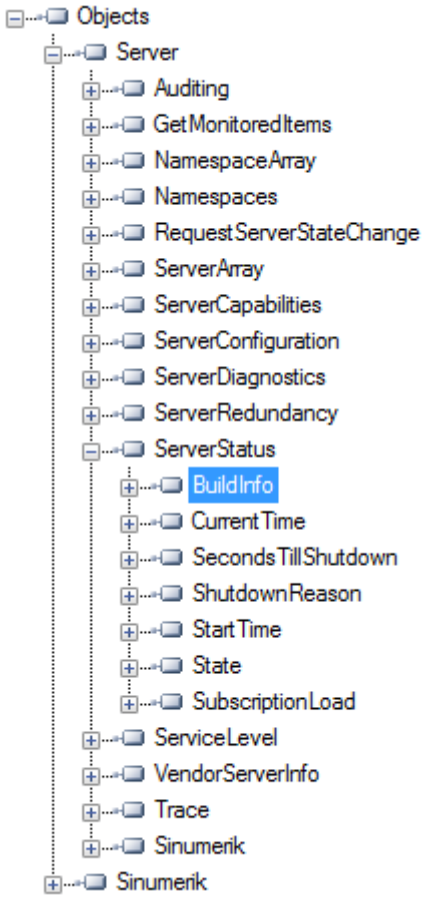


Figure 7-1 Diagnostics Information - Server Node

7.2 Status screen

Requirement

Note

To show the correct status of OPC UA server you must have at least one type of message encryption (128 bit or 256 bit) enabled.

Status screen

Additional to the server status information available via OPC UA, there is a SINUMERIK Operate screen, which shows the actual status of the OPC UA server.

To open the Status screen, select the operating area "Startup > Network" in SINUMERIK Operate, then press the "OPC UA" softkey. The OPC UA status screen is the first screen to be displayed.

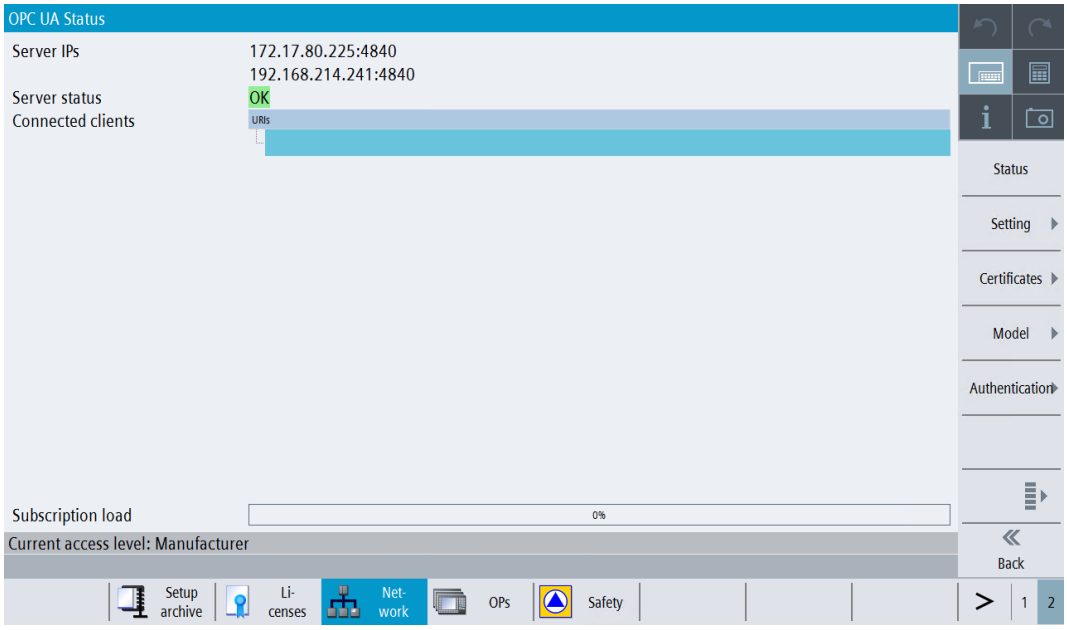


Figure 7-2 Status

Value	Description	Further explanation
Server IPs	Server IPs and ports of the company network, systems network or service network where the OPC UA server is accessible	
Server status	Possible status of the server: • Ok (server up and running) • Not activated (OPC UA server deactivated) • No connection can be set up (error within the OPC UA server) • No more sessions possible. All sessions are in use by other clients. The status screen cannot create a session.	There are too many sessions used by other clients. External clients are allowed to create 5 sessions with 828D and 10 sessions with 840D sl. The session limitation is 6 and 11 in the configuration file, respectively, to have one more session for the status client.
Connected clients	Clients which are connected to the server **Example**: • MD1EXMQC: remote PC of the client • SiemensAG:OpcUaTestsApp: URN of the application of the remote PC • 10788... Session ID • OpcUaTestConsole: Session Name	
Subscription load	Utilized capacity of the OPC UA server regarding possible subscriptions (see chapter Technical data (Page 163)), not the overall load.	

7.3 Diagnosis screen

Overview

Diagnosis screen offers support for troubleshooting and service for OEM with SIEMENS. Diagnosis functionalities are used only for service purpose.

From the Diagnosis screen user can:

- Activate or deactivate the OPC UA Server logging.
- Configure OPC UA Server logging.
- Reset the OPC UA Server to factory settings.
- Export the diagnosis data to an external data storage (for example, USB/Networkshare).

Note

Diagnosis softkey is visible by default only for manufacturer, service and user access levels.

OPC UA Diagnosis

1. Press the "OPC UA" softkey.
2. Press the extended softkey as shown in the below image.

   Note

   If the extended softkey is disabled then it means the OPC UA Server license is not active.

3. Press the "Diagnosis" softkey.

Note

The "Diagnosis" softkey will not be visible if OPC UA Server is not actiavted. User need to activate the OPC UA Server from the OPC UA settings screen.

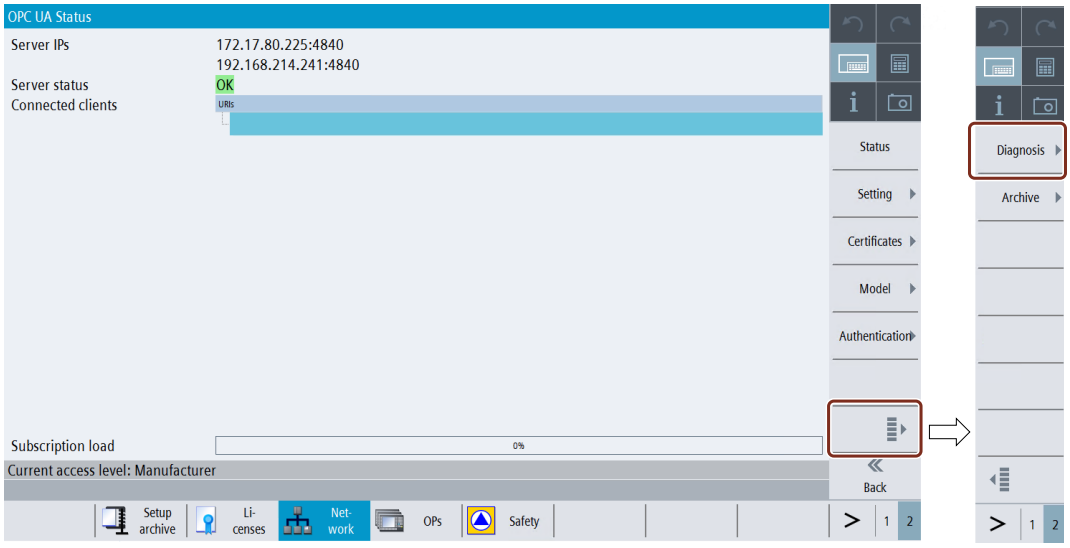


Figure 7-3 Softkey Diagnosis

4. The "OPC UA Diagnosis" dialog will appear. Then press the "Change" softkey.

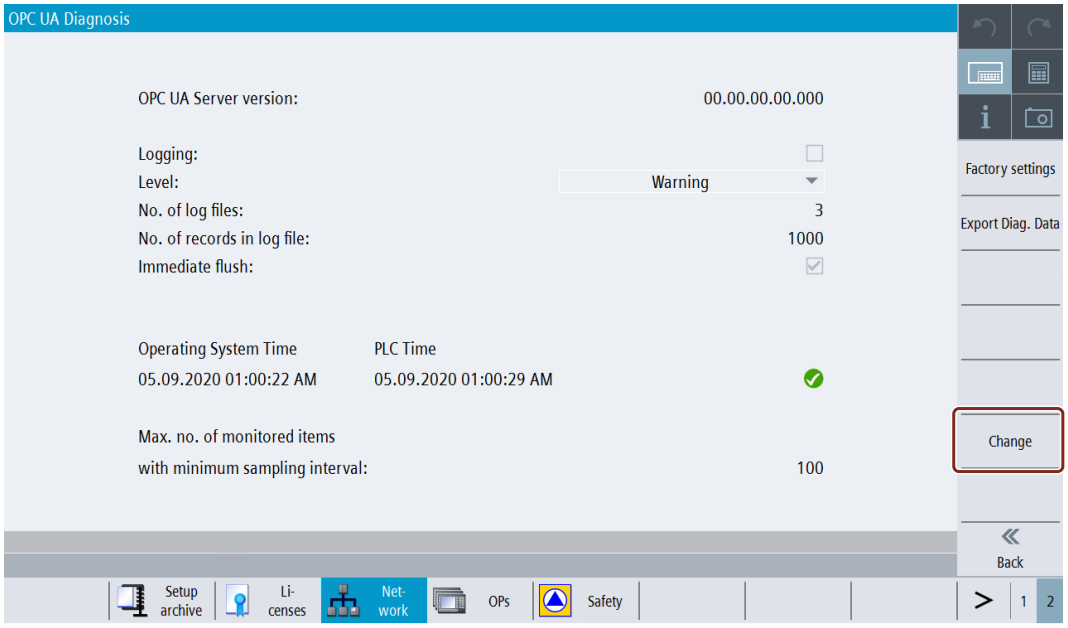


Figure 7-4 Softkey Change

5. Make the necessary settings for logging.

Note

The changes become effective only after the restart of the SINUMERIK Operate.

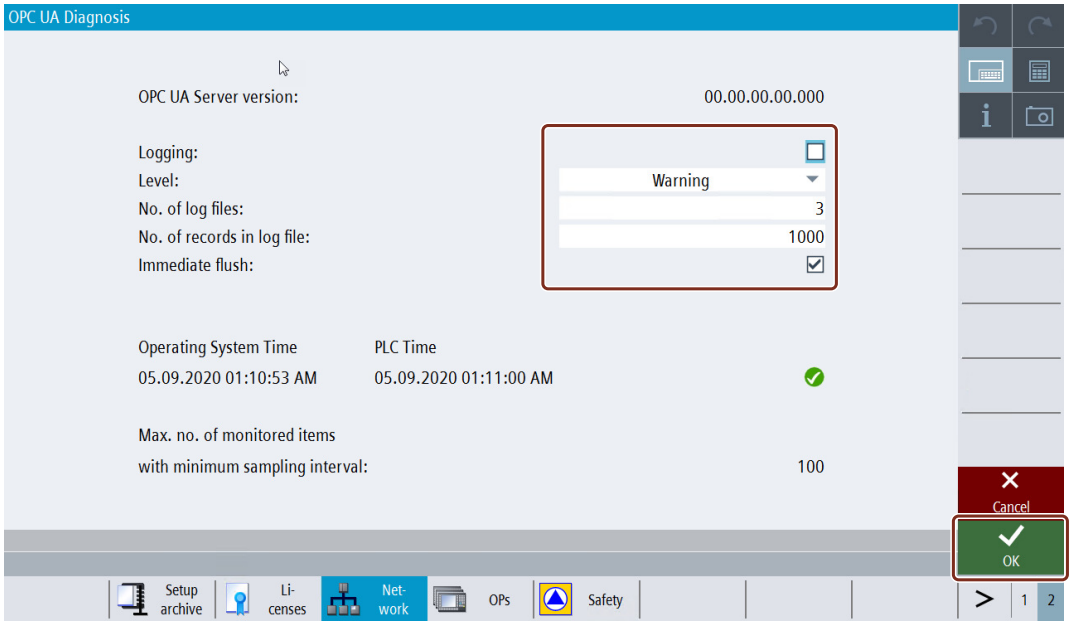


Figure 7-5 Activate Logging option

Field	Description
"OPC UA Server Version"	Shows the OPC UA Server version installed.
"Logging"	Place the checkmark to activate logging and remove the checkmark to deactivate it. By activating logging, it generates the log of the OPC UA Server.
"Level"	Select the type of level from the drop down list. The drop down list has the following types of level: • None • Error • Warning (by dafault) • System • Info • Debug • Content • All The log will be generated based on the selection of level type. No log will be generated if you have activated logging and selected "None" from the list.
"No. of log files"	Enter the no. of log files between 3 - 10. If the user selects 10, and the 10th log file is already generated, then it will replace the 1st log file.

Field	Description
"No. of records in log file"	Enter the no. of records in log file between 1000 - 99999. If the user selects 99999, and the 99999th record is already generated, then it will replace the 1st record.
"Immediate flush"	Place the checkmark to activate the immediate flush and remove the checkmark to deactivate it. By activating immediate flush, every record will be written immediately into the log file. This option should be used only for logging without delays.
"Operating System Time and PLC Time"	Operating System and PLC date and time are displayed. The tick icon indicates that the PLC time is in sync with the operating system (HMI Operate) time. If the date and time is not in sync, icon is shown and it indicates that time should be updated.
"Max. no. of monitored items with minimum sampling interval"	This field provides information about the max. no. of items which can be monitored with minimum sampling interval".

6. Then press "OK".
7. The changes become effective only after the restart of the SINUMERIK Operate.

Note

If the OPC UA server logging is activated for more than 30 days, then it will be automatically disabled on the next HMI restart.

Resetting the OPC UA Server to factory settings

This helps the user to reset the OPC UA configuration of the SINUMERIK device to its initial state. This would be helpful when the current OPC UA configuration is not valid and needs to be reset.

User shall use this as the last option to reconfigure the OPC UA server to its initial state. All settings, IP, Port, and certificates will be deleted and the default values will be restored.

After the restart of the SINUMERIK Operate, OPC UA server need to be activated again with necessary changes.

Note

Model files will not be deleted during this process.

1. Press the "OPC UA" softkey.
2. Press the extended softkey.
3. Press the "Diagnosis" softkey. The "OPC UA Diagnosis" dialog will appear.

4. Then press the "Factory settings" softkey.

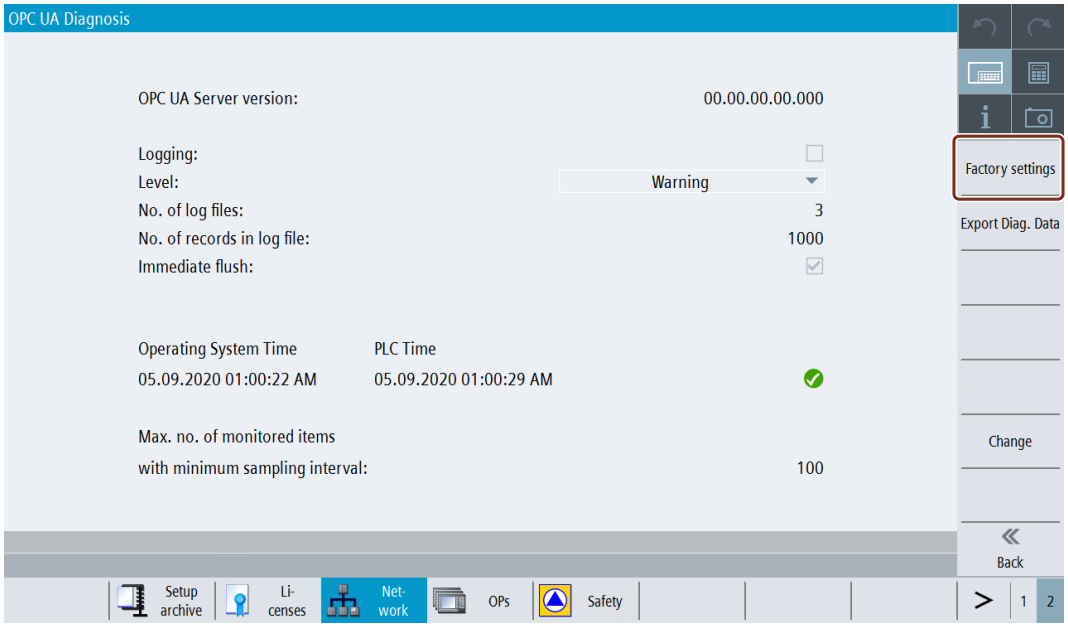


Figure 7-6 Softkey Factory Settings

5. The "Factory settings" popup window will appear.

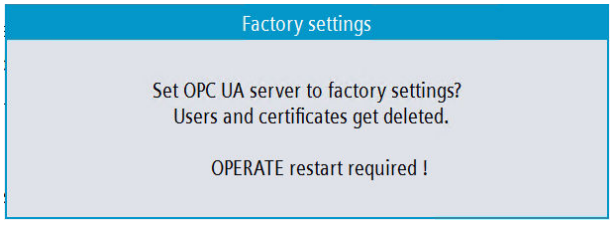


Figure 7-7 Factory settings popup

Note

If the user performs factory settings, the OPC UA Server will be reset to default setting. User need to enable the OPC UA Server again from the OPC UA settings screen (Page 21).

6. Then press "OK". A status message is shown at the bottom, "changes become effective after the restart of OPERATE".

Exporting diagnosis data to an external data storage

This feature exports the OPC UA configuration, log files and other diagnostic information from the SINUMERIK system, onto the selected USB or Network shared location.

This can be used to analyze details of behavior of the system or root cause of the situation in case of problems.

1. Press the "OPC UA" softkey.
2. Press the extended softkey.
3. Press the "Diagnosis" softkey. The "OPC UA Diagnosis" dialog will appear.

4. Then press the "Export Diag. data" softkey.

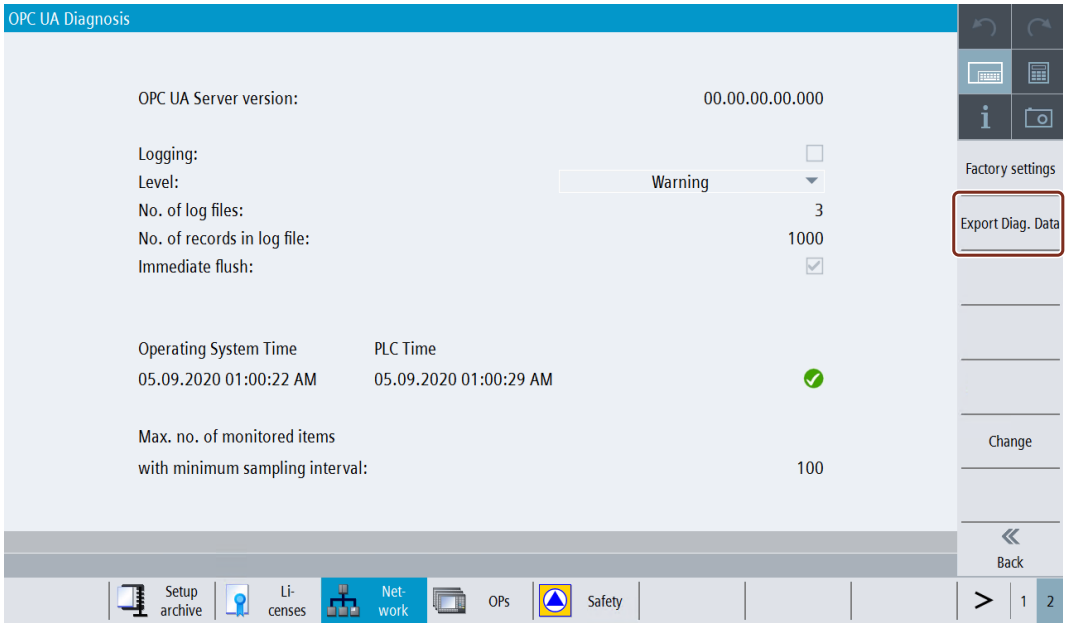


Figure 7-8 Softkey Export Diag data

5. The "Export OPC UA Diagnosis Data" popup window will appear.

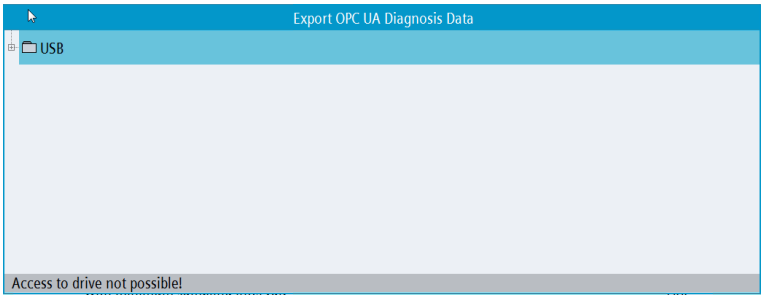


Figure 7-9 Export OPC UA Diagnosis data popup

6. Select either USB/Networkshare.
7. Then press "OK".
8. The diagnosis data will be saved to the folder (as selected USB/networkshare) in the format "OpcUaDiagnosisData_Year_Month_Day-Hour_Minute_Second",(for example: "OpcUaDiagnosisData_2020_06_22-11_12_56").

7.4 OPC UA Archiving

Overview

Archiving feature enables the user to generate a backup of OPC UA Server so that in case of need, all settings and data can be restored. Also, user can generate a setup archive for serial commissioning and update new machines with setup archive.

From Archiving screen user can:

- Generate OPC UA Server backup archive (i.e, full archive)
- Generate OPC UA Server setup archive for serial commissioning
- Restore backup archive
- Read in setup archive for serial commissioning

Prerequisite

OPC UA archive is only part of Operate archive, if the archive service in OPC UA has been done before. Therefore create an OPC UA backup first, before taking full backup of Operate.

OPC UA Server backup archiving

The user can generate a backup archive of OPC UA Server (including configuration, user management, models, and certificates) and restore it back when required. The OPC UA back up archive can only be restored on the same controller or the same SD card, since the server certificate is part of the backup.

Generating Archive

1. Press the "OPC UA" softkey.
2. Press the extended softkey as shown in the below image.

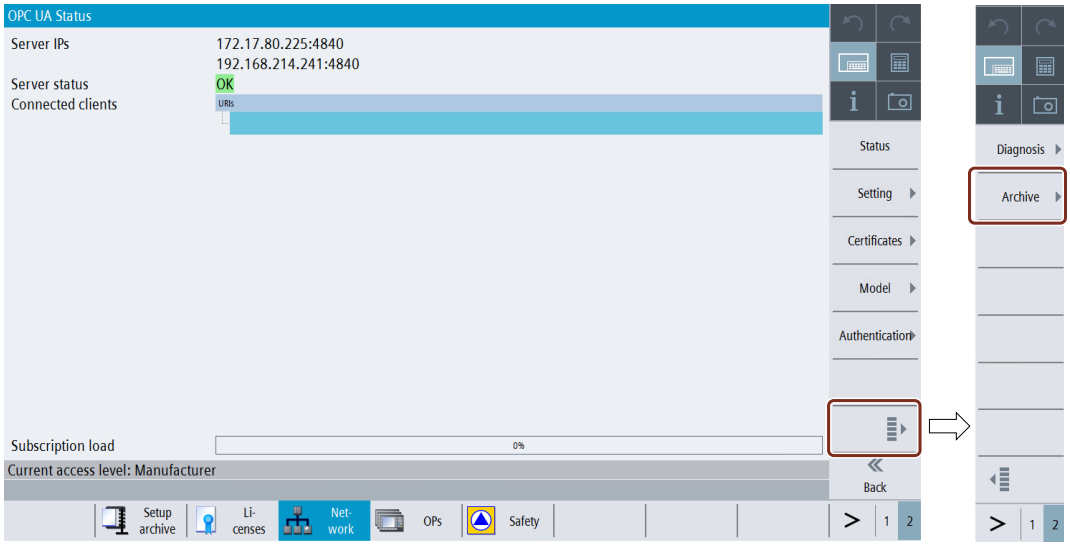


Figure 7-10 Softkey Extended

Note

If the OPC UA server license is not active, then the extended softkey is disabled.

3. Press the "Archive" softkey.

4. The "OPC UA Archives" dialog will appear. Select "All data of this OPC UA server (backup)" radio button under "Generate archive".

Note

The radio button "All data of this OPC UA server (backup)" is enabled by default only for manufacturer, service and user access levels.

Note

If additionally, you want the backup file to be copied to USB or network share, then select "Export additionally to USB/network share" check box. After Pressing "OK", a popup window appears. Select the location in the USB or network share where you want to save the backup file.

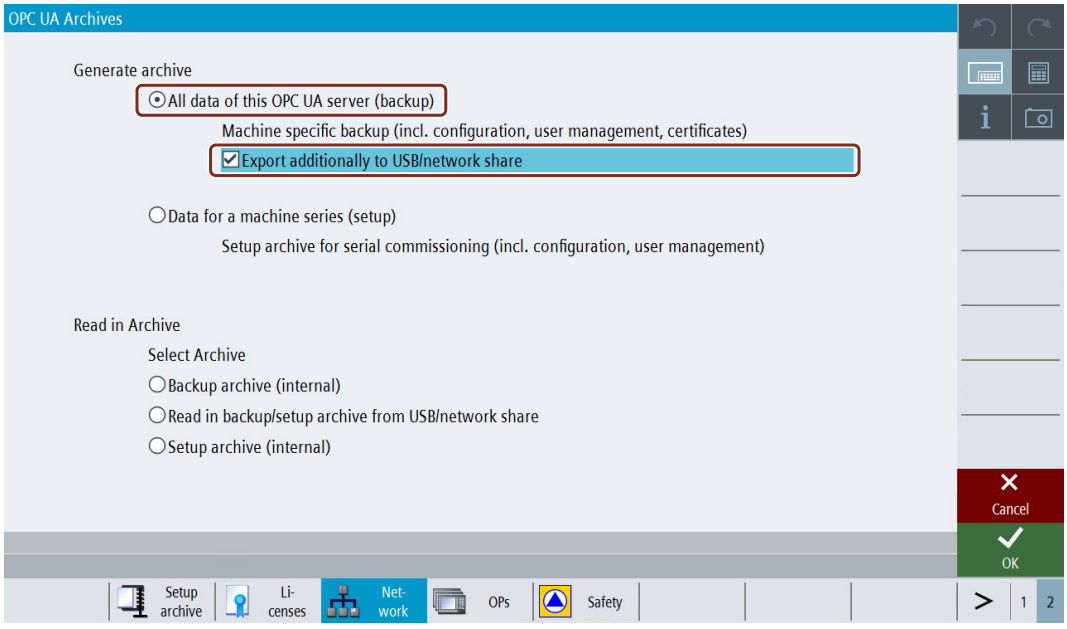


Figure 7-11 OPC UA Server generate backup archiving

5. Then press "OK". The popup window appears with message, "OPC UA archive generated successfully".

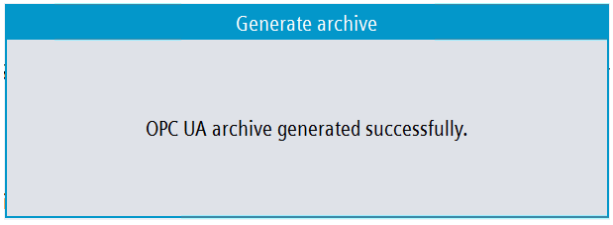


Figure 7-12 Generate archive popup

6. Press "OK". The backup file is saved automatically in the local folder (internal memory) and in the USB/network share as selected. The internal path for NCU will be "/card/user/sinumerik/hmi/cfg" and for PCU/IPC "C:\Program Files (x86)\Siemens\MotionControl/user/sinumerik/hmi/cfg".

Restoring backup archive

Note

- Backup archives can only be restored on the backed up target system.
- By restoring backup archive, all the current settings and data of the OPC UA Server will be replaced with the backup file data.

1. Select "Backup archive (internal)" radio button under "Read in Archive".

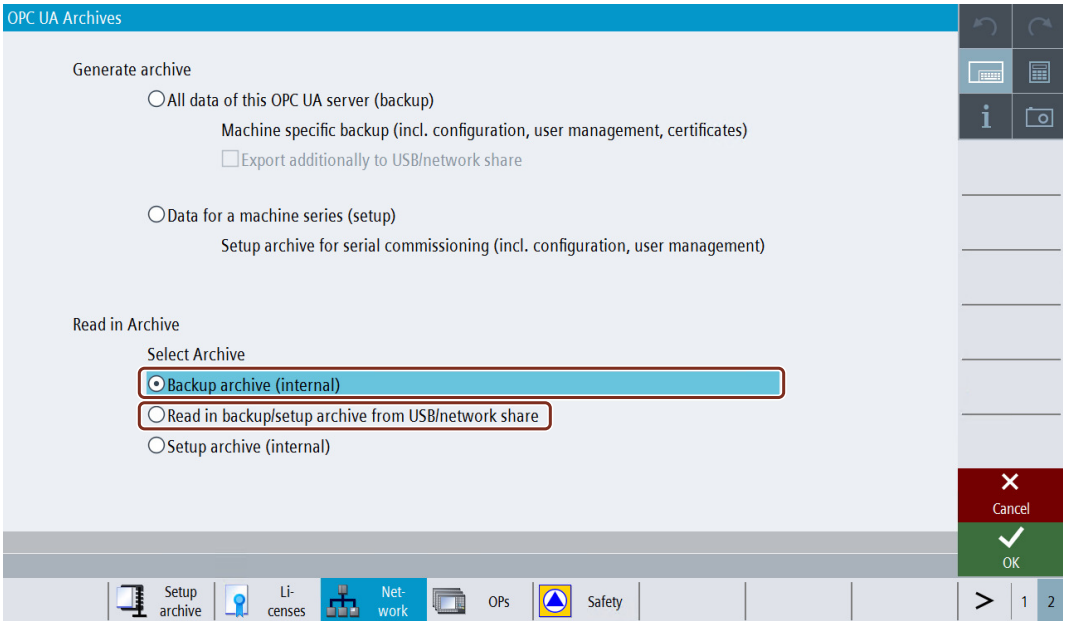


Figure 7-13 OPC UA Server restore backup archiving

In case, if you have saved and want to select the backup file from the USB/network share, then select "Read in backup/setup archive from USB/network share" radio button. After Pressing "OK", a popup window appears. Select the backup file from USB/network share.

2. Then Press "OK". With the valid input file, a popup window appears with message, "Read in completed successfully".

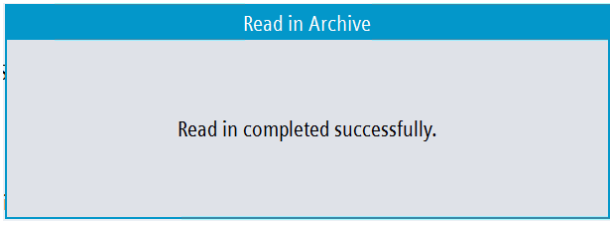


Figure 7-14 Read in archive success popup

3. Press "OK". The backup file is restored.

Note

The changes become effective only after the restart of the SINUMERIK Operate.

OPC UA Server setup archiving for serial commissioning

The user generates a setup archive of OPC UA Server for serial commissioning (including configuration, user management, and models) and update new machines with setup archive.

Generating Archive

1. Select "Data for a machine series (setup)" radio button under "Generate archive".

Note

This option is enabled only with manufacturer's access levels.

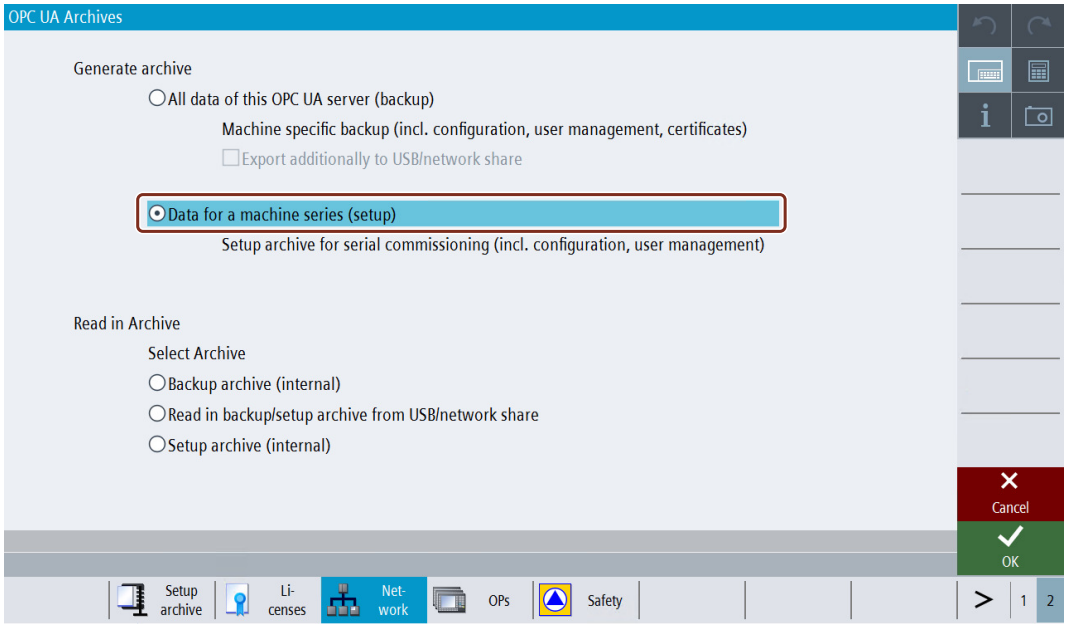


Figure 7-15 OPC UA Server generate setup archiving for serial commissioning

2. Press "OK". A popup window appears.
3. Select the location in the USB or network share where you want to save the setup file.
4. Then press "OK". The popup window appears with message, "OPC UA archive generated successfully".

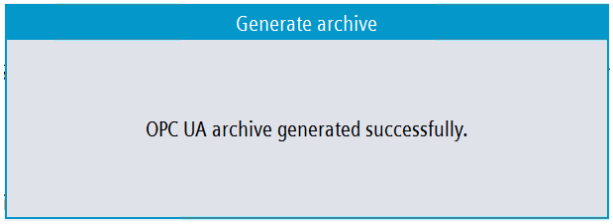


Figure 7-16 Generate archive success popup

5. Press "OK". The setup file is saved in the USB/network share as selected.

Setup archive

1. Select "Read in backup/setup archive from USB/network share" radio button under "Read in Archive".

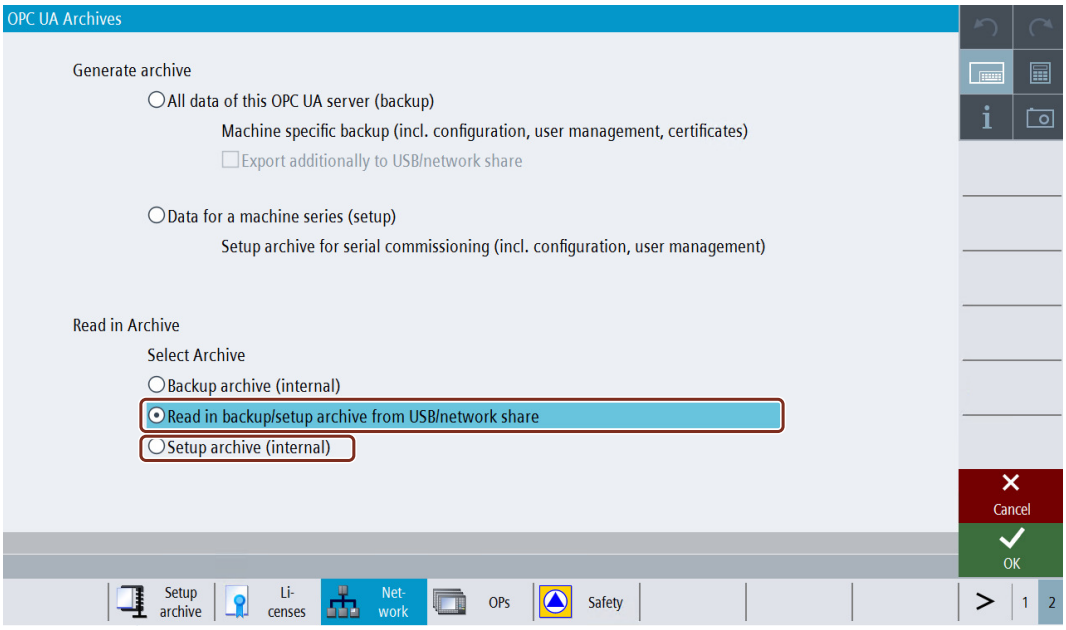


Figure 7-17 OPC UA Server setup archiving for serial commissioning

In case, if you have saved and want to select the setup file from local folder (internal memory), then select "Setup archive (internal)" radio button. The internal path for NCU will be "/card/user/sinumerik/hmi/cfg" and for PCU/IPC "C:\Program Files (x86)\Siemens \MotionControl/user/sinumerik/hmi/cfg".

Note

The "Setup archive (internal)" option is enabled only with manufacturer's access levels.

2. Press "OK". A popup window appears.

Figure 7-18 Setup archive USB_Networkshare popup

3. Select the setup file from USB/network share. Then Press "OK".

4. With the valid input file, a popup window appears with message, "Read in completed successfully".

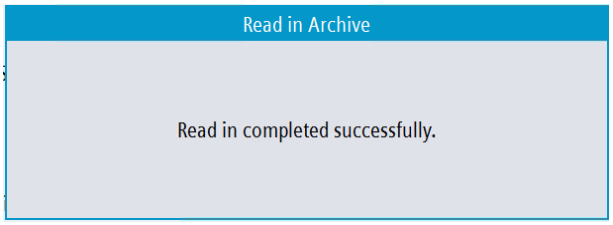


Figure 7-19 Read in archive success popup

5. Press "OK". The setup archive is completed.

Note

The changes become effective only after the restart of the SINUMERIK Operate.

Possible scenarios and error messages

Sl no.	Selection	Scenario description	Error message
1	Generate backup archive OR Generate setup archive	Generation of any archive, if completed without any issues.	OPC UA archive generated successfully.
2	Generate backup archive (internal memory)	If there is no sufficient memory available.	Insufficient memory on IPC/NCU.
3	Generate backup archive (on USB/ Netshare) OR Generate setup archive (on USB/ Netshare)	If there is no sufficient memory available.	Insufficient USB/ network memory
4	Generate backup archive (on USB/ Netshare) OR Generate setup archive (on USB/ Netshare)	If the selected location is write protected or not accessible.	No write permission on the selected medium.
5	Generate backup archive (on USB/ Netshare) OR Generate setup archive (on USB/ Netshare)	If the selected location is write protected or not accessible.	Access to drive is not possible.
6	Read in Backup archive Or Read in Setup archive	No valid OPC UA archive file is found in internal memory.	No OPC UA archive is available on internal memory
7	Read in Backup archive Or Read in Setup archive	No error in reading in file.	Read in completed successfully.

8	Read in Backup archive Or Read in Setup archive	If the selected file is not a valid OPC UA Archive or the file is tampered by editing.	Read in failed. Invalid file.
9	Read in Backup archive (external memory)	If backup archive is not from the same machine	Read in failed. Backup Archive is generated on different Sinumerik device.

7.5 OPC UA server version

OPC UA server version

OPC UA server version and OPC UA dialog version information can be found in SINUMERIK OPERATE version screen.

1. Open SINUMERIK OPERATE and choose operating area "Diagnostics". Press the softkey "Version".
2. Select “System extensions" and press softkey "Details".

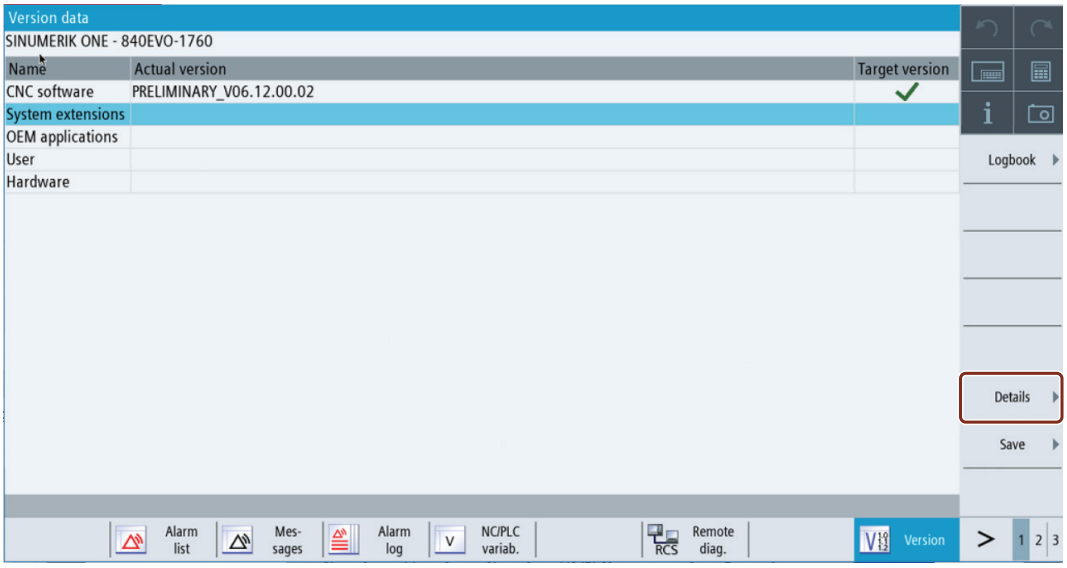


Figure 7-20 Version data

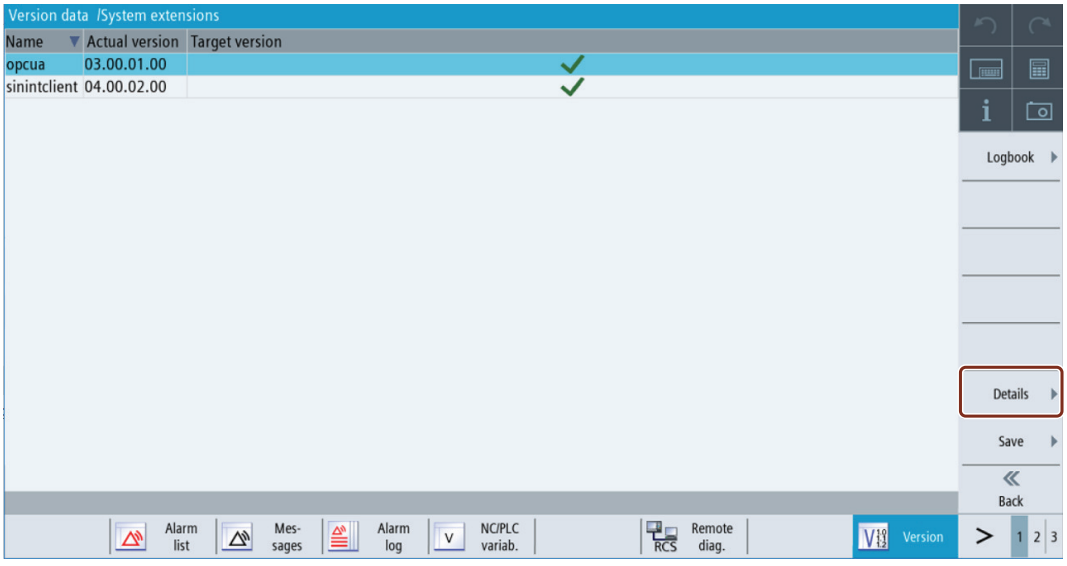


Figure 7-21 Version data / system extensions

The OPC UA entry is found.

3. Select the entry and press "Details" again to show more detailed information on OPC UA components.

Update of OPC UA server

8

8.1 Overview

Compatibility

This version of OPC UA server is supported by SINUMERIK 840D sl and SINUMERIK 828D.

An update process is possible with the following SINUMERIK software versions:

- Software line 4.5: with versions ≥ V4.5 SP4.
- Software line 4.7: with versions ≥ V4.7 SP2.
- Software line 4.8: with versions ≥ V4.8 SP1.
- Software line 4.9.

SINUMERIK Create MyConfig (CMC)

The necessary update (CMC) file can be provided by your regional SIEMENS office.

8.2 Compatibility

Compatibility

Below are the compatibility issues of OPC UA:

- Password
  The Password length has changed to min. 8 characters.
- User rights
  - The behavior in setting “SinuReadAll” and “SinuWriteAll” is different from previous versions.
  - Different from previous version is that removing the right “SinuReadAll” will remove all read rights. In previous versions additionally added read rights have not been deleted with removing “SinuReadAll”.
    Same applies to “SinuWriteAll”.

Note

If you face any other compatibility issues or for further details, refer to hotline (https://support.industry.siemens.com/cs/sc/2090/).

8.3 Installation of OPC UA server

Requirements

The installation procedure of the OPC UA server varies depending whether a PCU or a PPU/NCU is being used. The following operating systems are required:

- **PCU Base** and SINUMERIK Operate on **Windows 7 / Windows 10** systems
- SINUMERIK Operate on **NCU840D (embedded)**.

Below are the instructions for both options:

See also

Update of OPC UA server (Page 167)

8.3.1 Installation/Upgrade on a PCU/IPC

1. Load OPC UA software (OpcUaDeployWindows_XXX.XXX.exe) on USB stick.
2. Start PCU in the service mode.
3. Insert USB stick in USB port of operator panel.
4. Start Windows Explorer.
5. Navigate to .exe file and execute it.
6. Follow the installation instructions.
7. After successful installation, restart the PCU.

Note

If OPC UA was active before the installation, users and access rights are being preserved.

8.3.2 Installation/Upgrade a PPU/NCU

Note

Different installation procedure for 828D / V4.5

Please not that the server update procedure for 828D with CNC software version V4.5 varies from the standard process below (see chapterUpdate of OPC UA server (Page 167)).

1. Load OPC UA software (OpcUaDeployLinux_XXX.XXX.usz) on USB stick.
2. Insert USB stick in USB port of NCU/PPU.
3. Switch off NCU/PPU and switch it on again.

4. Follow the installation instructions.
5. After successful installation, restart the NCU/PPU.

Note

If OPC UA was active before the installation, users and access rights are being preserved.

Technical data

9

Technical data

Description	Value	
Number of sessions [1]	828D	5
	840 D sl	10
Number of subscriptions [2]	828D	5
	840D sl	10
Maximum samples / second [3]	828D	500 1/s
	840D sl	1000 1/s
Maximum no. of monitored items [4]	controller specific	
Min. sampling interval [3]	100 ms	
Sampling intervals	{100, 250, 500, 1000, 2500, 5000} ms	
Min. publishing interval	100 ms	
Publishing intervals	{100, 250, 500, 1000, 2500, 5000} ms	
Max. number of users	20	
Max. lifetime interval (LifeTime Count)	1 h	
Session timeout	60 s	
Max. monitored items queue size (Subscription Queue size) [5]	10000	

[1] Session = Connection of a client to a server

[2] Subscription = In an existing session a subscription is a functionality for monitoring data items.

[3] Accessible communication performance / quantity structure depends on the working load of the control

[4] The maximum no. of monitored items depends on the update rate of all monitored items over all sessions and a controller specific performance index.

[5] Total queue size over all subscriptions and all monitored items

Calculating maximum no. of monitored items

The maximum number of monitored items depends on the update rate of all monitored items and a performance index of the controller. The maximum number of monitored items can be calculated as shown below:

Max. no. monitored items = **(Performance Index / 1000)** x **Sampling Rate (ms)**

Performance Index

- 828D = 500
- 840D sl = 1000

See also

Monitored items (Page 103)

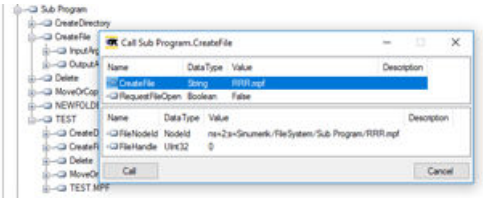
Trouble shooting

11

11.1 Frequently asked questions (FAQs)

Topic	Question	Possible solution
OPC UA client has no connection	In spite of correct commissioning my OPC UA client cannot connect. What can I do?	If no connection is possible, though you have operated the commissioning of the OPC UA server thoroughly, it is recommended to restore factory settings of the OPC UA server. Proceed as follows: • Deactivate OPC UA in the setting dialog • Switch off IPC/NCU and on again • Activate OPC UA again in the setting dialog • Switch off IPC/NCU and on again
	The server cannot be found by the client. What can I do?	• Check whether the IP address of the networking dialog is compatible to those of the OPC UA dialog. • If the IP addresses are not compatible, press "Change" in the OPC UA setting dialog. The new addresses will be directly transferred into the setting dialog. • Confirm with "Ok" and restart the SINUMERIK. The connection the server should function properly now.
	The OPC UA server status shows OK but the client is not able to connect. What can I do?	• Power Off/On, the control in order to activate all necessary firewall settings (e.g.: port number changed).
OPC UA export diagnosis data	How can I export OPC UA diagnosis data?	Refer to topic, "Exporting diagnosis data to an external data storage" under chapter, "Diagnosis screen (Page 142)".
OPC UA client cannot connect as certificate user	• Certificate user is created • Certificate for certificate user is trusted • OPC UA client cannot connect as certificate user	Please check date and time of the target system. In case the target system time is not within the period of validity (valid from – valid to) of the client certificate, the connection gets refused (BadIdentityTokenRejected).
OPC UA server is not accessible after update	After a server update, the server cannot be accessed anymore. What can I do?	• Check that the time on the HMI is set correctly. • Check the validity periods of the servers and client certificates. • Check whether port is open in the firewall.

File Sysytem

Topic	Question	Possible solution
File System	How to use "CreateDirectory" method?	The OPC UA server can create a folder with any extension or with no extensions in the USB drive, network share, and local drive. However in the NC drive, we can create an extension with "DIR" only.
	How to use "CreateFile" method?	The "CreateFile" method is used to create a new file. The created file can be written using the "Write" method of the FileType. The OPC UA server can create file without extension in the USB drive, network share, and local drive but not in the NC memory. 
	How to use "Delete" method?	• The "Delete" method is used to delete a file/directory. The OPC UA server will not allow to delete the file if the file is opened for the file operation. You must close the file handle to delete the file. In case of directory, all the file and directory objects below the directory to delete are deleted recursively. • A file which is selected for execution or a folder which contains the selected file are not allowed to be moved. However if the file is moved there is a possibility that an empty file will be created.
	How to use "MoveOrCopy " method?	• The "MoveOrCopy" method is used to move or copy a file/directory to another directory or to rename a file/directory. • The OPC UA server can move any file or folder without extension in the USB drive, network share, and local drive but not in the NC memory. In the NC memory, a folder with the extension "DIR" can only be allowed to be moved to the NC memory. • The OPC UA server will not allow to move the folder if the file is opened for the file operation. • A file which is selected for execution or a folder which contains the selected file, are not allowed to be moved. However if the file is moved there is a possibility that an empty file will be created.
	How to use "Open " method?	When a client opens a file, it gets a file handle that is valid while the session is open. Clients shall use the "Close" method to release the handle when they do not need access to the file anymore. Clients can open the same file several times for read.
	How to use "Read " method?	The "Read" method is used to read a part of the file starting from the current file position. The file position is advanced by the number of bytes read. The data contains the returned data of the file. If the ByteString is empty, it indicates that the end of the file is reached.

Topic	Question	Possible solution
	How to use "Write " method?	The "Write" method is used to write a part of the file, starting from the current file position. The file position is advanced by the number of bytes written. When the client session is closed, all the open file handled will be closed for the respective session. In this scenario, if there is any existing file opened with write mode or append mode, the current data will be lost.
	How to use "Close " method?	The "Close" method is used to close a file represented by a FileType. When a client closes a file, the handle becomes invalid.
	How to use "GetPostion " method?	The "GetPosition" method is used to provide the current position of the file handle. If a "Read" or "Write" method is called, it starts at that position.
	How to use "SetPosition " method?	The "SetPosition" method is used to set the current position of the file handle. If a "Read" or "Write" method is called, it starts at that position. If the position is higher than the file size, the position is set to the end of the file.
	Does OPC UA standard file system support 1:N constellation?	No, only the default machine name is mapped (target system IPC only).

See also

Technical support (https://support.industry.siemens.com/cs/sc/2090/)

11.2 Reference to OPC UA error code

You can find all relevant information on error codes at Github (https://github.com/OPCFoundation/UA-Nodeset/blob/master/DotNet/Opc.Ua.StatusCodes.cs).

Technical Support

Country-specific telephone numbers for technical support are provided in the Internet at the following address (https://support.industry.siemens.com/cs/sc/2090/) in the "Contact" area.

If you have any technical questions, use the online form in the "Support Request" area.

Annex

A

A.1 840D sl documentation overview

You will find extensive documentation on the functions of SINUMERIK 840D sl from version 4.8 SP4 at 840D sl documentation overview (https://support.industry.siemens.com/cs/ww/en/view/109766213).

You can display the documents or download them in PDF or HTML5 format.

The documentation is divided into the following categories:

- User: Operating
- User: Programming
- Manufacturer/Service: Configure
- Manufacturer/Service: Commissioning
- Manufacturer/Service: Functions
- Safety Integrated
- SINUMERIK Integrate / MindApp
- Information and training