SIEMENS

SINUMERIK

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

Configuration Manual

Valid for:

OPC UA server Version 2.1

08/2018
6FC5397-1DP41-0BA1

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
Division Digital Factory
Postfach 48 48
90026 NÜRNBERG
GERMANY

Document order number: 6FC5397-1DP41-0BA1
Ⓟ 08/2018 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.

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.

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 46))
- Transfer of part programs (see chapter File system (Page 70))
- Support for File and Folder Objects
- Event based provision of SINUMERIK alarms and messages from HMI, NC and PLC (see chapter Alarms (Page 56))
- Methods for selection of part programs from the NC file system (see chapter Select (Page 77)) and tool management (see chapter Tool management (Page 81))
- Multi language support for the alarm and warning messages.

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 39)).

See also

Certificate handling (Page 24)

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. If a Windows operating system is used, the OPC UA server is also accessible as LocalHost.	
	Thin Client	If a Thin Client is used, the OPC UA server is accessible after successful licensing and activation via 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" (X1) interface of the PCU / IPC. In this case the OPC UA server is not accessible via the X130 interface of the NCU.

Application scenario

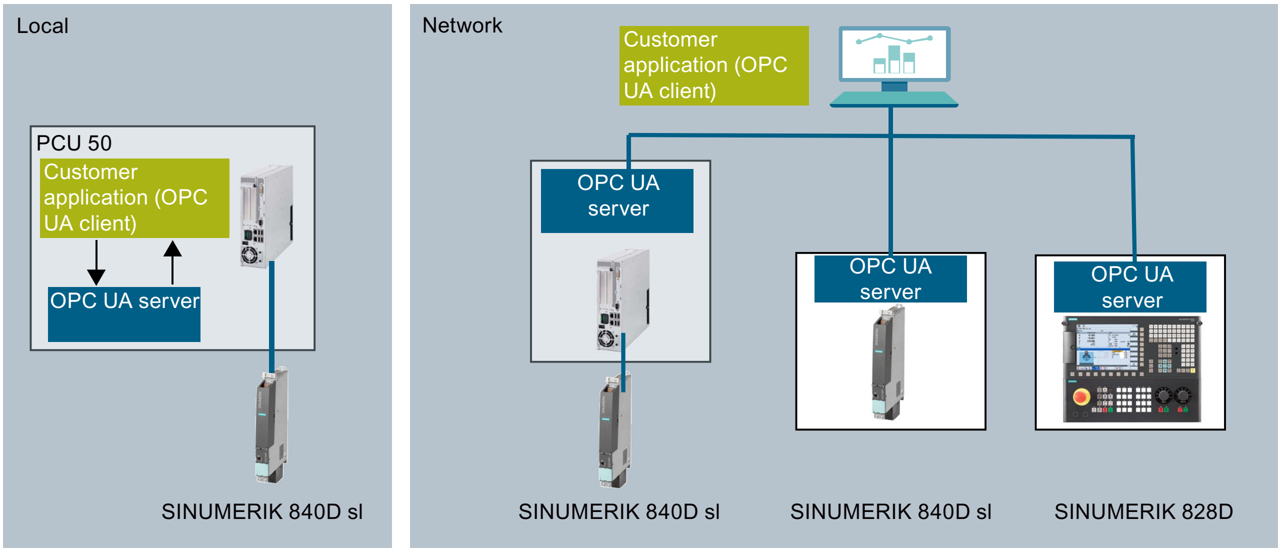


Figure 1-1 Application scenario

1.4 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 (parameter assignments) 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 Industrial security

Note

Industrial security

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:

Industrial security (http://www.siemens.com/industrialsecurity)

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

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed at:

Industrial security (http://www.siemens.com/industrialsecurity)

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, malware 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.
- Protect the drive against unauthorized changes by activating the "know-how protection" drive function.

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. Please refer to chapter User administration (Page 39), especially chapter List of rights (Page 42).

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).

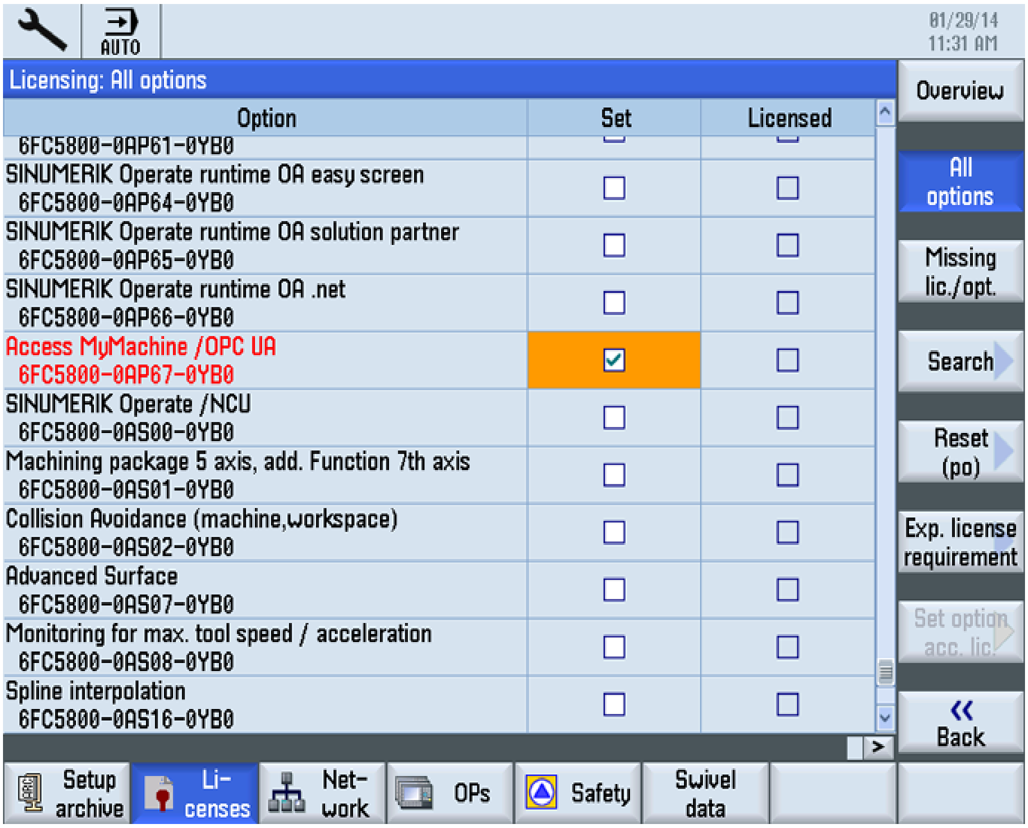
Prerequisites

- OPC UA requires SINUMERIK Operate.
- OPC UA requires an OPC UA license (6FC5800-0AP67-0YBO).
- 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.



Licensing: All options

Option	Set	Licensed
6FC5800-0AP61-0YB0	□	□
SINUMERIK Operate runtime OA easy screen 6FC5800-0AP64-0YB0	□	□
SINUMERIK Operate runtime OA solution partner 6FC5800-0AP65-0YB0	□	□
SINUMERIK Operate runtime OA .net 6FC5800-0AP66-0YB0	□	□
Access MyMachine /OPC UA 6FC5800-0AP67-0YB0	☑	□
SINUMERIK Operate /NCU 6FC5800-0AS00-0YB0	□	□
Machining package 5 axis, add. Function 7th axis 6FC5800-0AS01-0YB0	□	□
Collision Avoidance (machine,workspace) 6FC5800-0AS02-0YB0	□	□
Advanced Surface 6FC5800-0AS07-0YB0	□	□
Monitoring for max. tool speed / acceleration 6FC5800-0AS08-0YB0	□	□
Spline interpolation 6FC5800-0AS16-0YB0	□	□

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

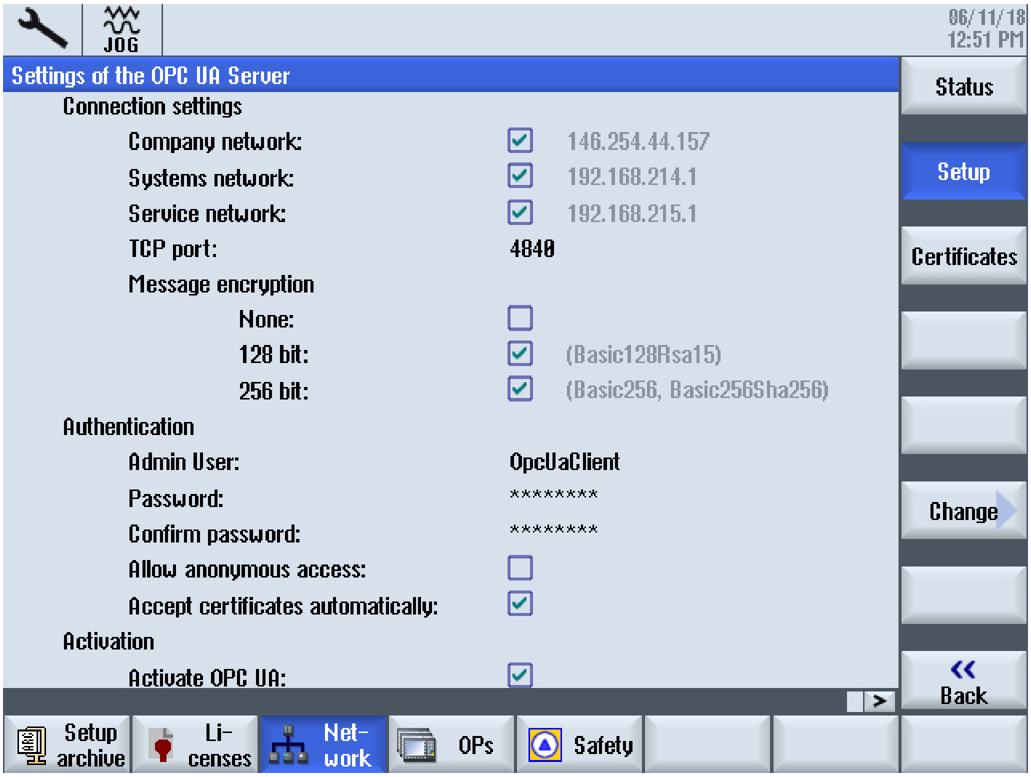
The certificate needed for secure OPC UA communication is automatically created during the first run-up. The start date of the validity period is set to the current date. The validity period is 20 years.

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).

Executing the OPC UA configuration dialog

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

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



Settings of the OPC UA Server

Connection settings

Company network: ☑ 146.254.44.157
Systems network: ☑ 192.168.214.1
Service network: ☑ 192.168.215.1
TCP port: 4840
Message encryption
None: □
128 bit: ☑ (Basic128Rsa15)
256 bit: ☑ (Basic256, Basic256Sha256)

Authentication

Admin User: OpcUaClient
Password: ********
Confirm password: ********
Allow anonymous access: □
Accept certificates automatically: ☑

Activation

Activate OPC UA: ☑

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

<table>
<tr><th>Group</th><th>Setting</th><th colspan="2">Description</th></tr>
<tr><td rowspan="7">Connection settings</td><td>• Company network
• Systems network (machine network)
• Service network</td><td colspan="2">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.
It is possible to activate or deactivate an interface from OPC UA server point of view.</td></tr>
<tr><td>TCP Port</td><td colspan="2">TCP port at which the OPC UA server should be available.
Standard configuration: 4840
<b>Note!</b>
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 rowspan="5">Message encryption</td><td colspan="2">It can be chosen which security endpoints should be offered from the server</td></tr>
<tr><td><b>Setting</b></td><td><b>Standard configuration</b></td></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>
<tr><td rowspan="5">Authentication</td><td>Admin User</td><td colspan="2">User name of the administrator. The administrator can add or delete users and assign or delete user authorizations.</td></tr>
<tr><td>Password</td><td colspan="2">Password of the administrator.</td></tr>
<tr><td>Confirm Password</td><td colspan="2">Enter the password again for confirmation.</td></tr>
<tr><td>Allow anonymous access</td><td colspan="2">Standard configuration: Deactivated
Anonymous access is only recommended for commissioning.</td></tr>
<tr><td>Accept certificates automatically</td><td colspan="2">Standard configuration: Activated
If this option is set, all client certificates are automatically accepted. For manual acceptance, please refer to chapter Certificate handling.</td></tr>
<tr><td>Activation</td><td>Activate OPC UA</td><td colspan="2">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

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.

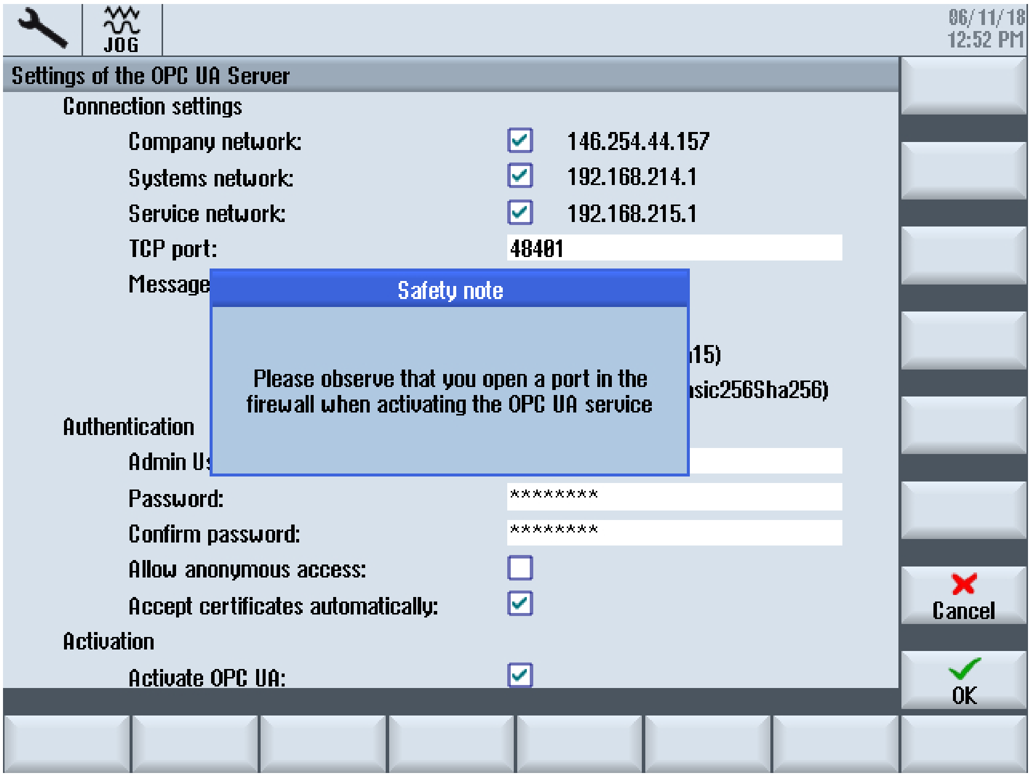
The German Federal Office for IT Security (BSI) (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/International/GSK_15_EL_EN_Draft.pdf?__blob=publicationFile&v=2) provides additional rules for creating secure passwords.

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

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



Settings of the OPC UA Server

Connection settings

Company network: ☑ 146.254.44.157

Systems network: ☑ 192.168.214.1

Service network: ☑ 192.168.215.1

TCP port: 48401

Message

15)

isic256Sha256)

Safety note

Please observe that you open a port in the firewall when activating the OPC UA service

Authentication

Admin Us

Password: ********

Confirm password: ********

Allow anonymous access: □

Accept certificates automatically: ☑

Activation

Activate OPC UA: ☑

Figure 3-3 Security message for opening the 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. 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 the SINUMERIK Operate is necessary on the PCU 50.

3.4 Certificate handling

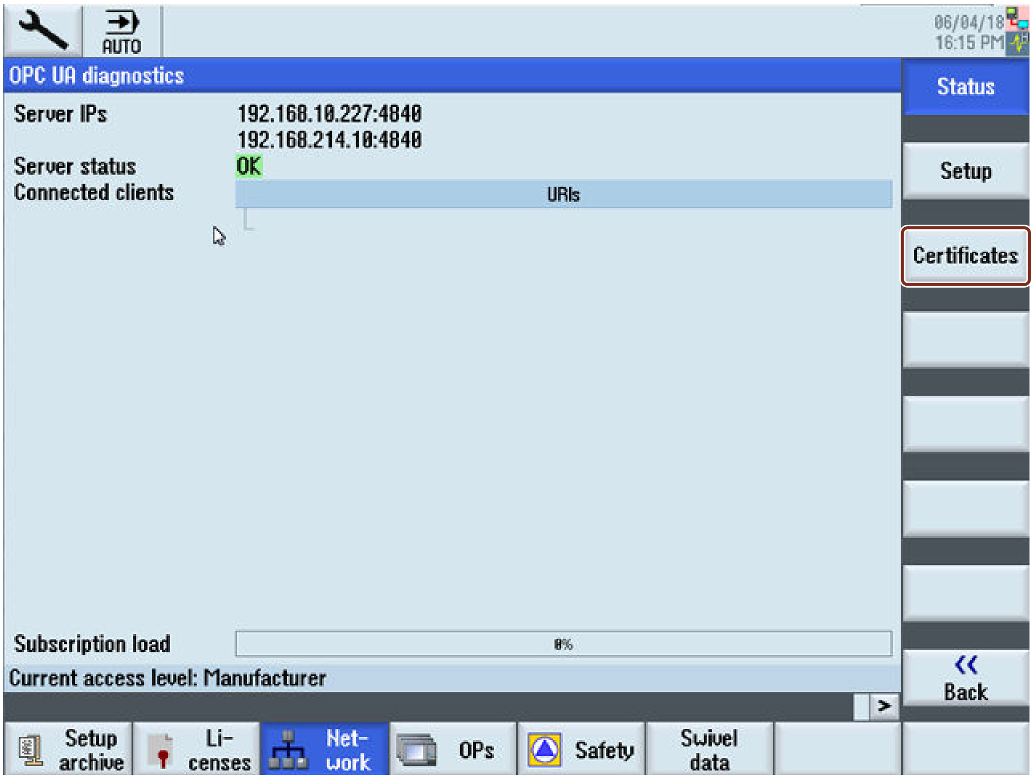
3.4.1 Overview

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 SINUMERIK 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".



OPC UA diagnostics

Server IPs 192.168.10.227:4840
192.168.214.10:4840
Server status OK
Connected clients URIs

Subscription load 0%
Current access level: Manufacturer

Figure 3-4 Softkey Certificates

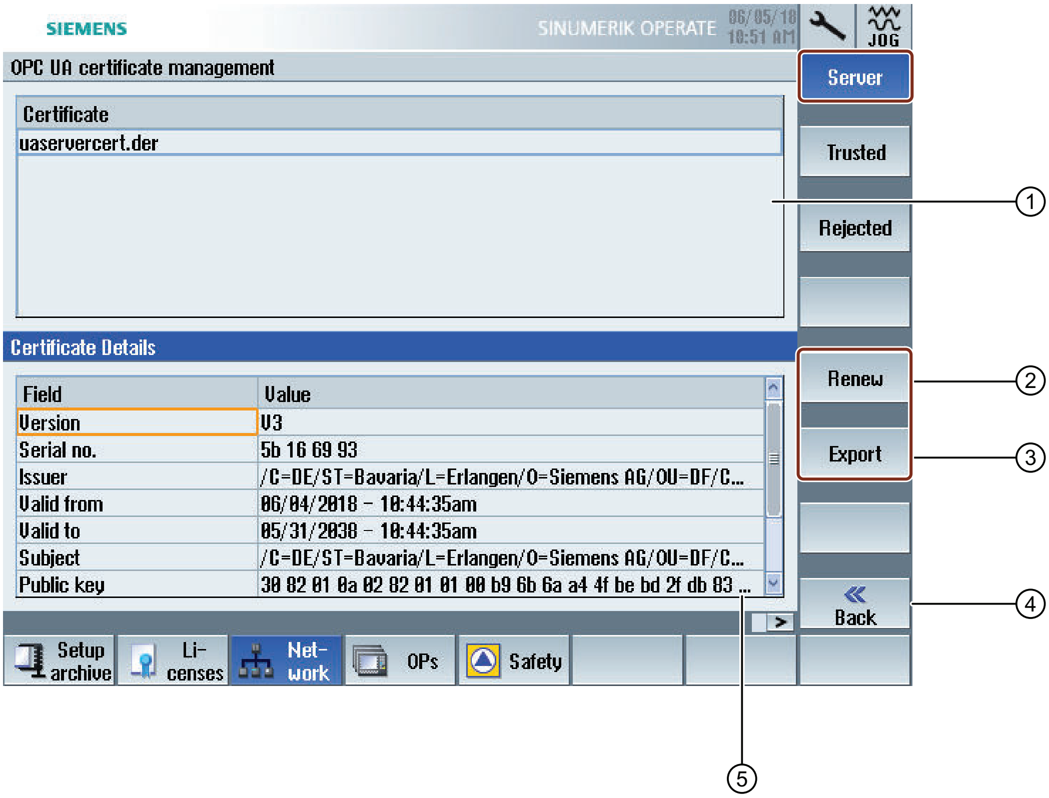
Operations

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



OPC UA certificate management

Certificate
uaservercert.der

Certificate Details

Field	Value
Version	V3
Serial no.	5b 16 69 93
Issuer	/C=DE/ST=Bavaria/L=Erlangen/O=Siemens AG/OU=DF/C...
Valid from	06/04/2018 - 10:44:35am
Valid to	05/31/2038 - 10:44:35am
Subject	/C=DE/ST=Bavaria/L=Erlangen/O=Siemens AG/OU=DF/C...
Public key	30 82 01 0a 02 82 01 01 00 b9 6b 6a a4 4f be bd 2f db 83 ...

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 an USB 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 3-5 Server Certificate

Renewing server certificates

If the server certificate is no longer valid or will expire soon, it is possible to renew the server certificate. 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 host name should be mentioned in the server certificate

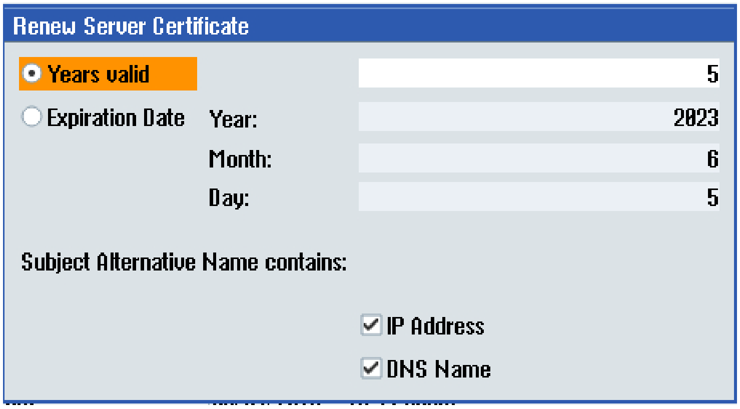
  Note

  Many clients will need the IP address in the certificate for validation. If the server will be addressed by hostname (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 host 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 host name should be written in the server certificate.



Renew Server Certificate

● Years valid: 5

○ Expiration Date Year: 2023
Month: 6
Day: 5

Subject Alternative Name contains:

☑ IP Address
☑ DNS Name

Figure 3-6 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

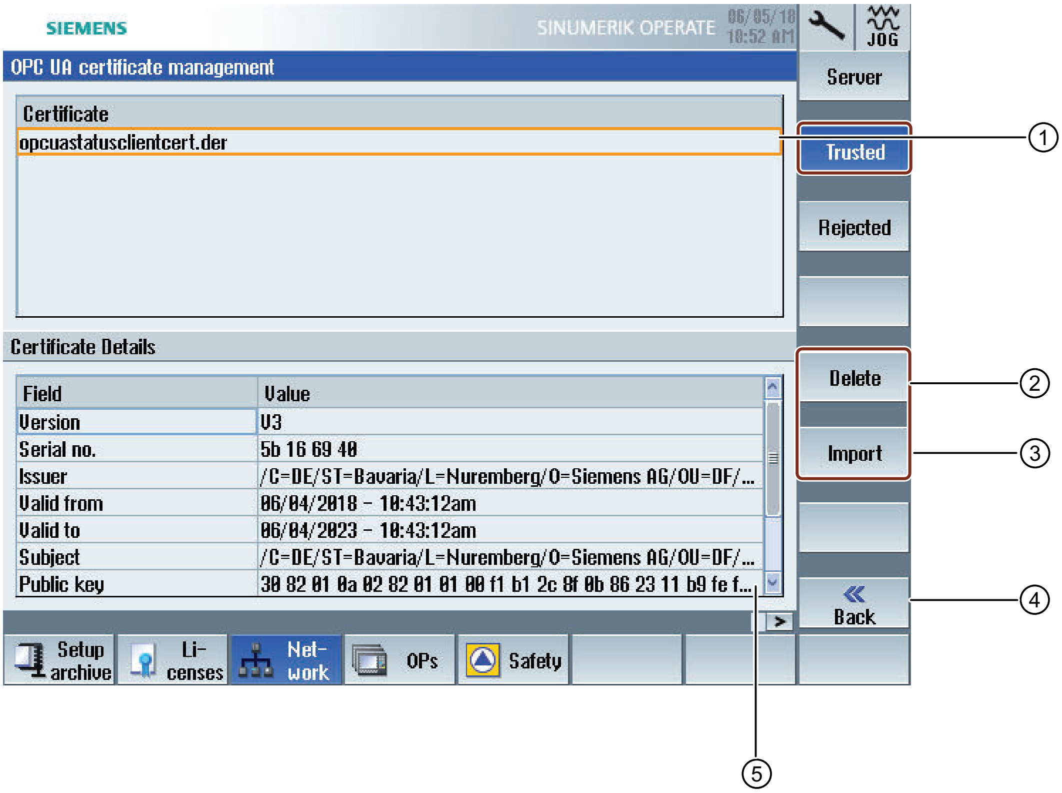
For an offline preparation of the connection to the server, you can export the server certificate. After that the certificate can be imported and trusted on the client side.

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



OPC UA certificate management

Certificate
opcuastatusclientcert.der

Certificate Details

Field	Value
Version	V3
Serial no.	5b 16 69 40
Issuer	/C=DE/ST=Bavaria/L=Nuremberg/O=Siemens AG/OU=DF/...
Valid from	06/04/2018 - 10:43:12am
Valid to	06/04/2023 - 10:43:12am
Subject	/C=DE/ST=Bavaria/L=Nuremberg/O=Siemens AG/OU=DF/...
Public key	30 82 01 0a 02 82 01 01 00 f1 b1 2c 8f 0b 86 23 11 b9 fe f...

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.

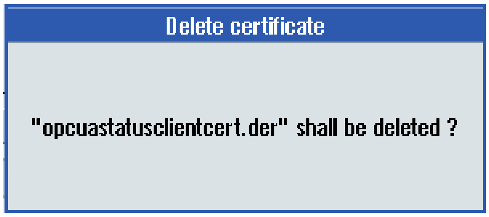
④ You can leave the OPC UA dialogs.

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. On touchscreens simply touch the screen.

Figure 3-7 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:



"opcuastatusclientcert.der" shall be deleted ?

Figure 3-8 Delete certificate

Pressing the softkey "Cancel" will do no action and return to "Rejected" 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

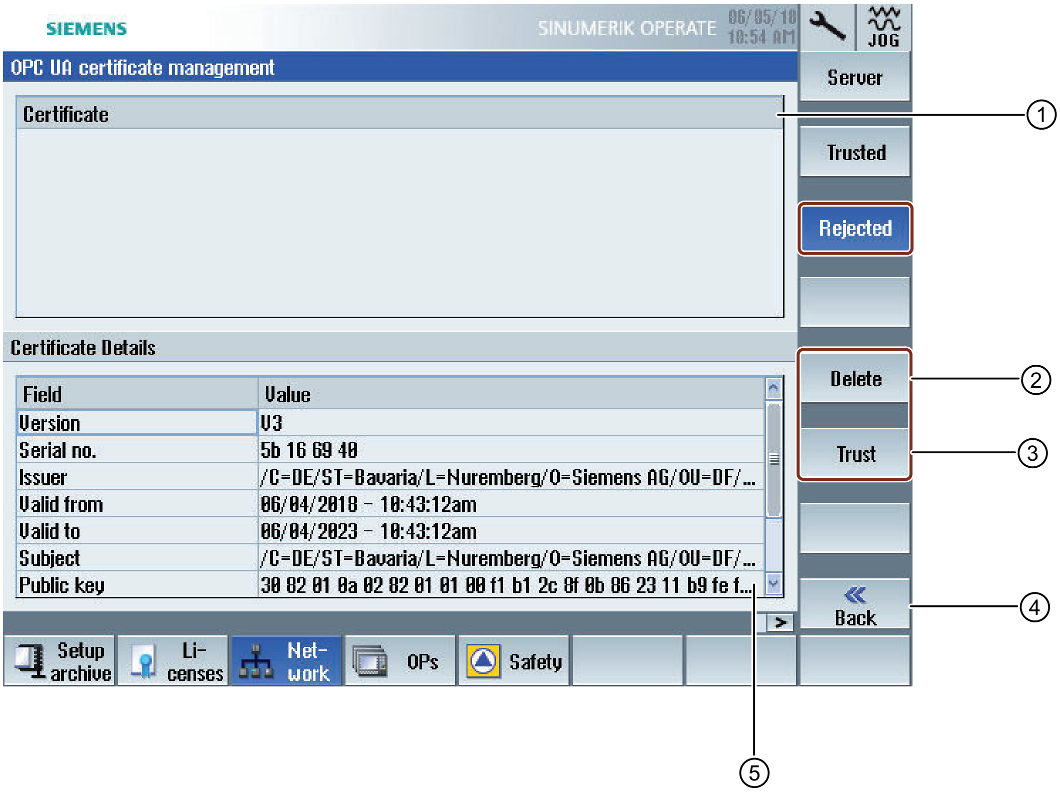
Keep in mind, that only certificates with the file extension "*.der" are accepted.

Note

To use a certificate for authentication it must not only be trusted, but also connected to a user using the method "AddCertificateUser".

3.4.3.2 Rejected certificates

Overview



Certificate

Certificate Details

Field	Value
Version	V3
Serial no.	5b 16 69 40
Issuer	/C=DE/ST=Bavaria/L=Nuremberg/O=Siemens AG/OU=DF/...
Valid from	06/04/2018 - 10:43:12am
Valid to	06/04/2023 - 10:43:12am
Subject	/C=DE/ST=Bavaria/L=Nuremberg/O=Siemens AG/OU=DF/...
Public key	30 82 01 0a 02 82 01 01 00 f1 b1 2c 8f 0b 86 23 11 b9 fe f...

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.

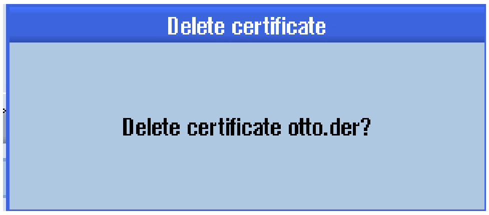
④ You can leave the OPC UA dialogs.

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. On touchscreens simply touch the screen.

Figure 3-9 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:



Delete certificate

Delete certificate otto.der?

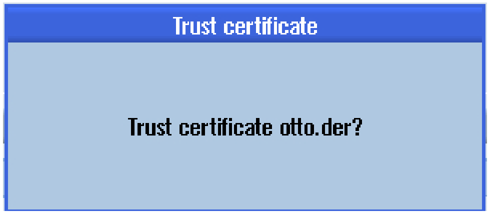
Figure 3-10 Delete cerficate

Pressing the softkey "Cancel" will do no action and return to the "Trusted" 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.



Trust certificate

Trust certificate otto.der?

Figure 3-11 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.

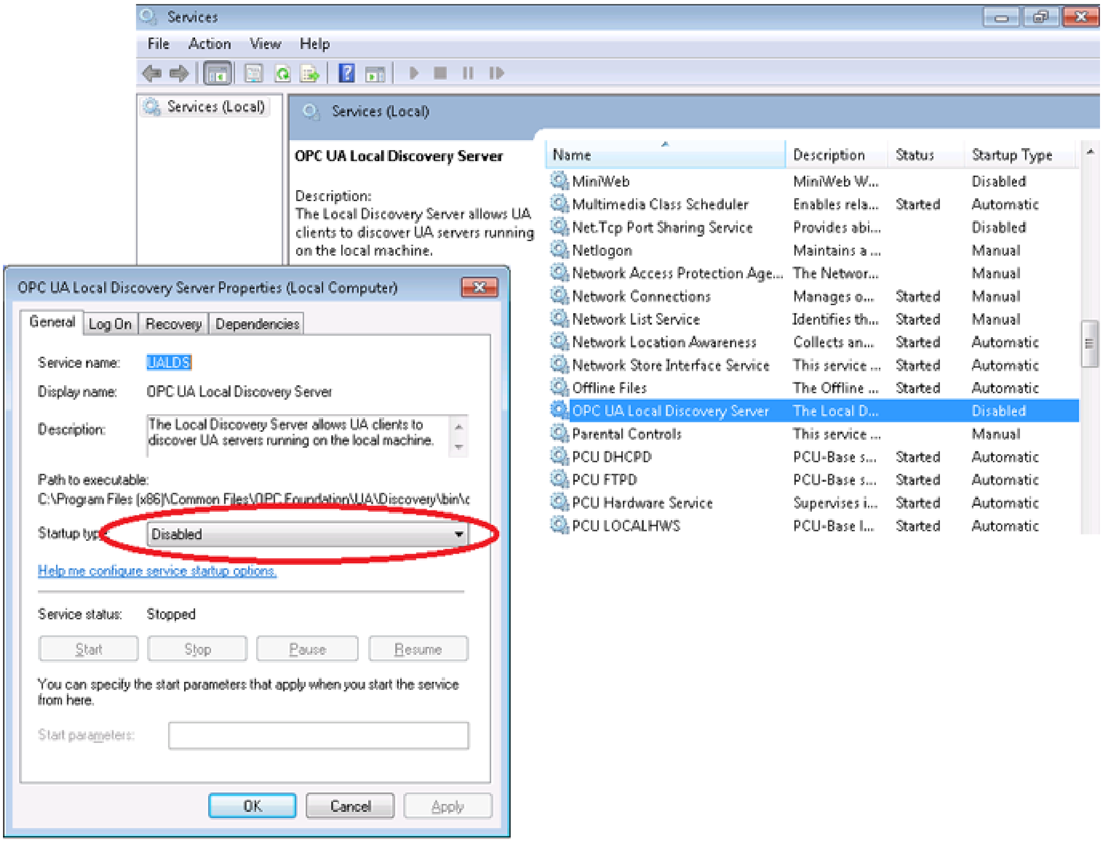
Installation

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, you must deactivate this service.

Note

If the service "OPC UA Local Discovery Server" is active, the SINUMERIK 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.



OPC UA Local Discovery Server

Description:
The Local Discovery Server allows UA clients to discover UA servers running on the local machine.

Name	Description	Status	Startup Type
MiniWeb	MiniWeb W...		Disabled
Multimedia Class Scheduler	Enables rela...	Started	Automatic
Net.Tcp Port Sharing Service	Provides abi...		Disabled
Netlogon	Maintains a ...		Manual
Network Access Protection Age...	The Networ...		Manual
Network Connections	Manages o...	Started	Manual
Network List Service	Identifies th...	Started	Manual
Network Location Awareness	Collects an...	Started	Automatic
Network Store Interface Service	This service ...	Started	Automatic
Offline Files	The Offline ...	Started	Automatic
OPC UA Local Discovery Server	The Local D...		Disabled
Parental Controls	This service ...		Manual
PCU DHCPD	PCU-Base s...	Started	Automatic
PCU FTPD	PCU-Base s...	Started	Automatic
PCU Hardware Service	Supervises i...	Started	Automatic
PCU LOCALHWS	PCU-Base l...	Started	Automatic

OPC UA Local Discovery Server Properties (Local Computer)

Service name: UALDS

Display name: OPC UA Local Discovery Server

Description: The Local Discovery Server allows UA clients to discover UA servers running on the local machine.

Path to executable:
C:\Program Files (x86)\Common Files\OPC Foundation\UA\Discovery\bin\c

Startup typ Disabled

Help me configure service startup options.

Service status: Stopped

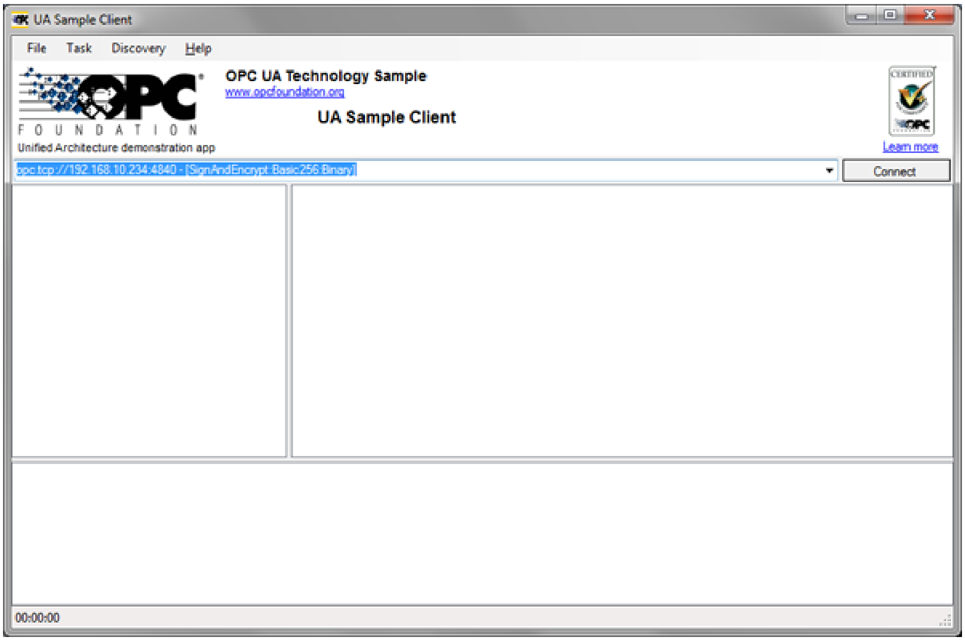
You can specify the start parameters that apply when you start the service from here.

Start parameters:

Figure 3-12 Deactivating the "OPC UA Local Discovery Server" service on PCU 50

Procedure

1. Start the OPC UA "Sample client".

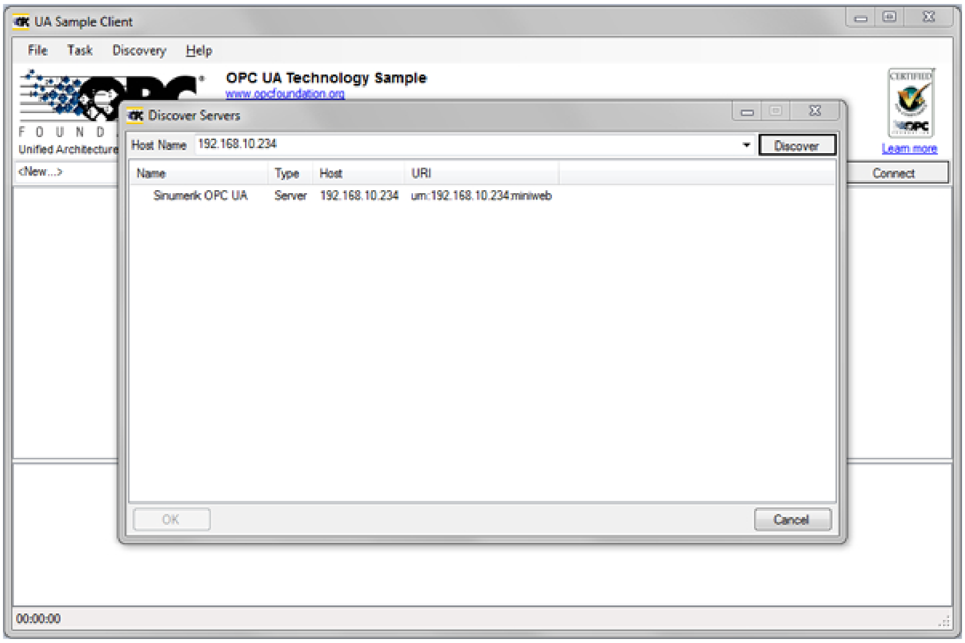


opc.tcp://192.168.10.234:4840 - [SignAndEncrypt:Basic256:Binary]

00:00:00

Figure 3-13 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.



Host Name 192.168.10.234

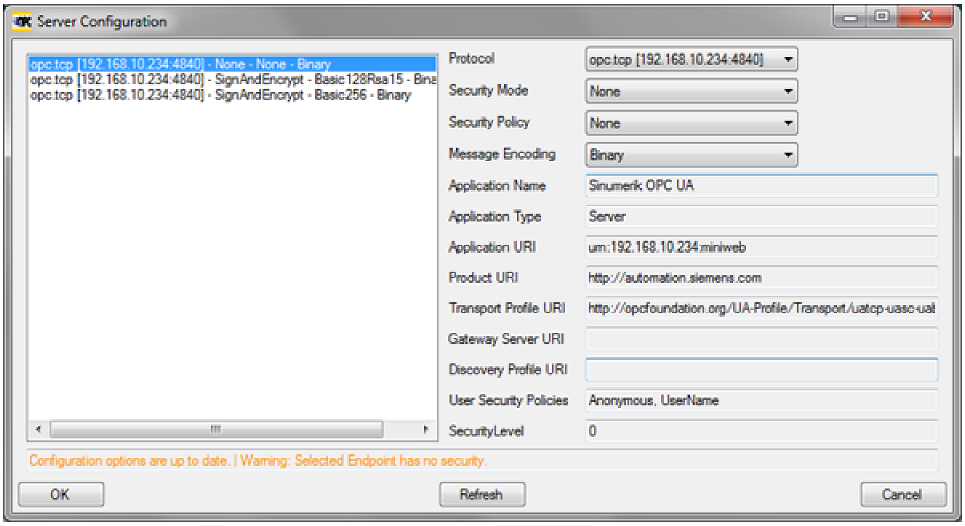
Name	Type	Host	URI
Sinumerik OPC UA	Server	192.168.10.234	urn:192.168.10.234:miniweb

00:00:00

Figure 3-14 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".

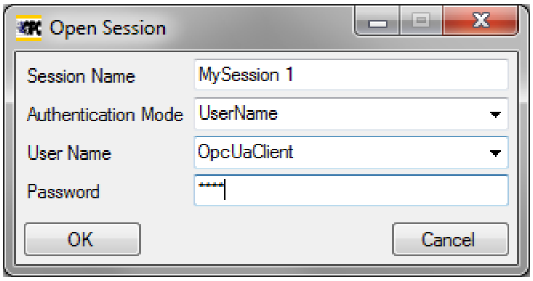


opc.tcp [192.168.10.234:4840] - None - None - Binary
opc.tcp [192.168.10.234:4840] - SignAndEncrypt - Basic128Rsa15 - Bina
opc.tcp [192.168.10.234:4840] - SignAndEncrypt - Basic256 - Binary

Protocol: opc.tcp [192.168.10.234:4840]
Security Mode: None
Security Policy: None
Message Encoding: Binary
Application Name: Sinumerik OPC UA
Application Type: Server
Application URI: urn:192.168.10.234:miniweb
Product URI: http://automation.siemens.com
Transport Profile URI: http://opcfoundation.org/UA-Profile/Transport/uatcp-uasc-uat
Gateway Server URI:
Discovery Profile URI:
User Security Policies: Anonymous, UserName
SecurityLevel: 0

Configuration options are up to date. | Warning: Selected Endpoint has no security.

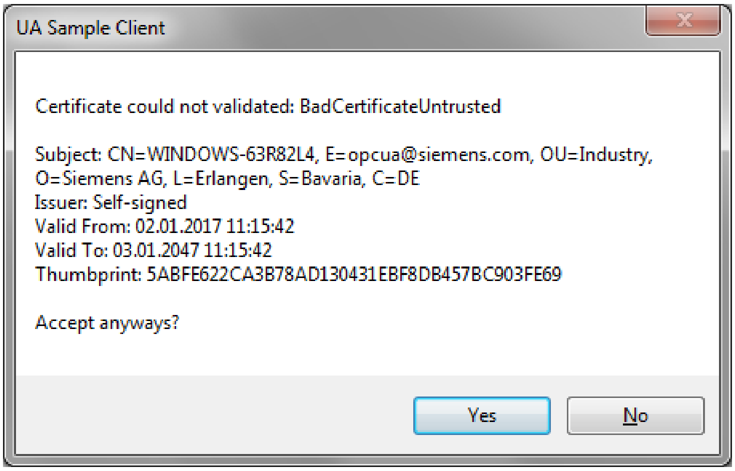
Figure 3-15 Server configuration



Session Name: MySession 1
Authentication Mode: UserName
User Name: OpcUaClient
Password: ****

Figure 3-16 User Identity

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



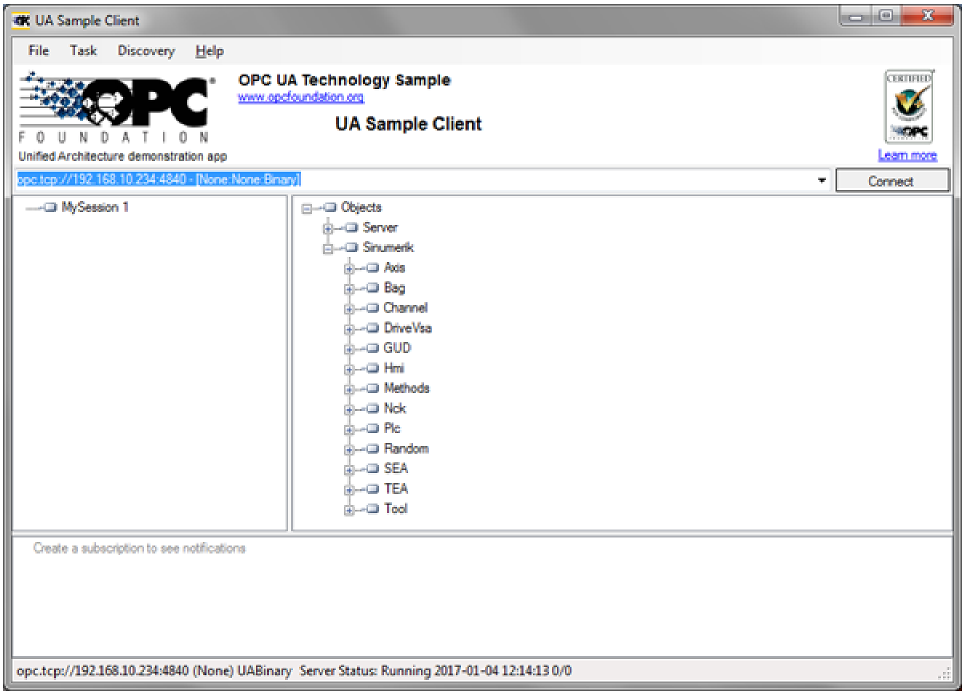
Certificate could not validated: BadCertificateUntrusted

Subject: CN=WINDOWS-63R82L4, E=opcua@siemens.com, OU=Industry, O=Siemens AG, L=Erlangen, S=Bavaria, C=DE
Issuer: Self-signed
Valid From: 02.01.2017 11:15:42
Valid To: 03.01.2047 11:15:42
Thumbprint: 5ABFE622CA3B78AD130431EBF8DB457BC903FE69

Accept anyways?

Figure 3-17 Certificate

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



opc.tcp://192.168.10.234:4840 - [None:None:Binary]

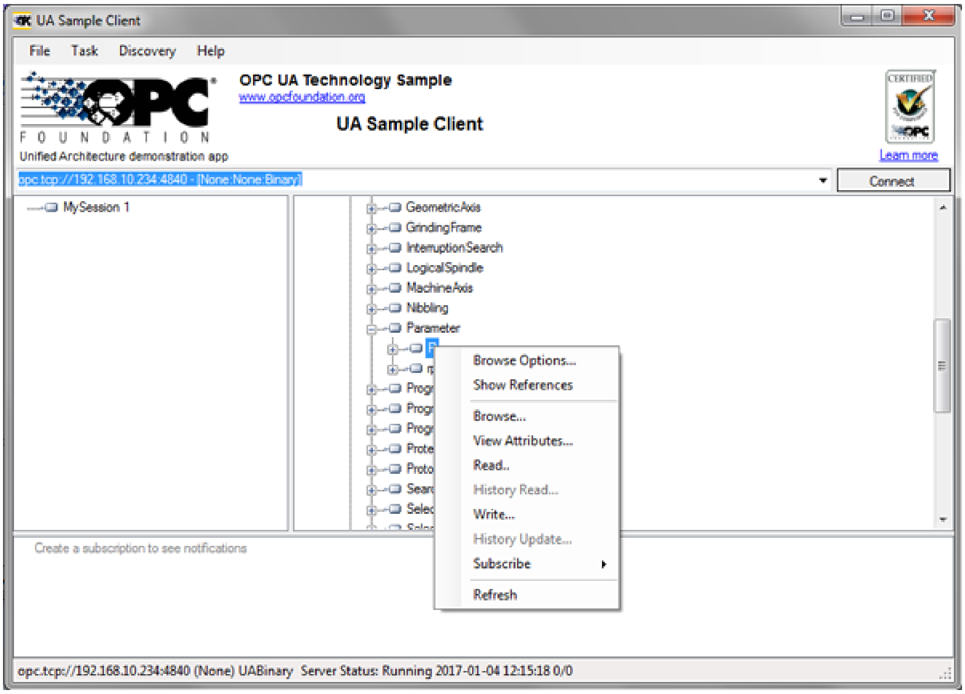
Create a subscription to see notifications

opc.tcp://192.168.10.234:4840 (None) UABinary Server Status: Running 2017-01-04 12:14:13 0/0

Figure 3-18 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:

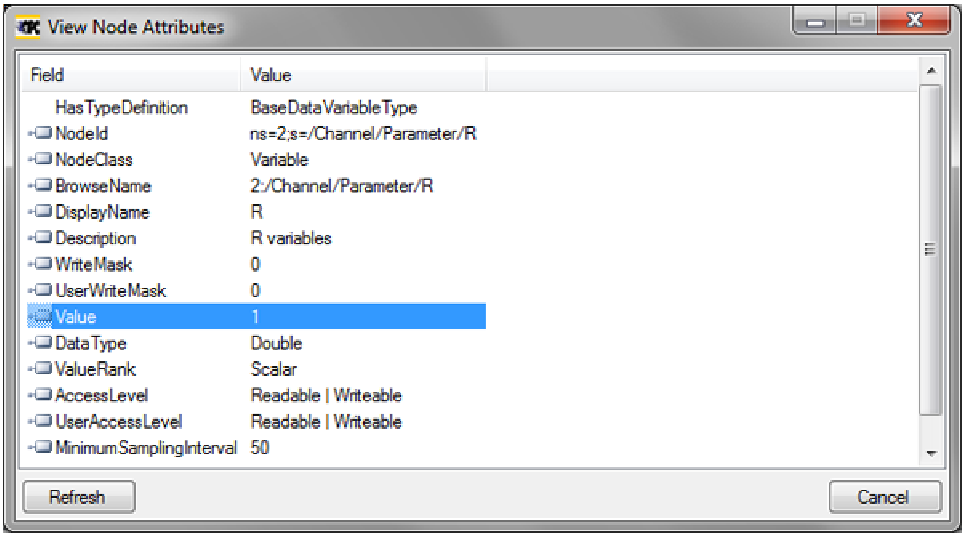
– E.g. read, write, setup monitoring



opc.tcp://192.168.10.234:4840 (None) UABinary Server Status: Running 2017-01-04 12:15:18 0/0

Figure 3-19 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.



Field	Value
HasTypeDefinition	BaseDataVariableType
NodeId	ns=2;s=/Channel/Parameter/R
NodeClass	Variable
BrowseName	2:/Channel/Parameter/R
DisplayName	R
Description	R variables
WriteMask	0
UserWriteMask	0
Value	1
DataType	Double
ValueRank	Scalar
AccessLevel	Readable | Writeable
UserAccessLevel	Readable | Writeable
MinimumSamplingInterval	50

Figure 3-20 Viewing node attributes

User administration 4

4.1 Overview

The admin can add/delete users and 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 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 rights As an administrator you are fully responsible for the administration of users and their rights. Any error in the administration process can lead to the misuse of 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 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/remove users/rights if you are connected as administrator. If you call the methods with a different user, you will receive the message "BadInvalidArgument".

4.2 User management

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

Table 4-1 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.	

4.3 Rights management

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

Table 4-2 Methods for user administration

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

4.4 List of rights

Below is the list of rights a user is assigned:

Table 4-3 List of rights

Method	Description	
GiveUserAccess	Sets the specified access rights for a user. The rights below can be combined in any combination.	
	Input Arguments:	
	User	User name which is to given the rights
	Realm	The access rights to be set as a string. If a user wants to set several 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 (and ReadVar method), read access
	"RandomWrite"	Random (and WriteVar method), write access
	"SinuReadAll"	All of the read access operations mentioned
	"SinuWriteAll"	All of the write access operations mentioned
	"ApWrite"	Allows to call method "Select"
	Example: GiveUserAccess ("MyUser", "GudRead; PlcWrite") Sets the read access for user data for the "MyUser" user and sets the write access for the PLC.	

Functionality 5

5.1 Overview

Overview

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:

- **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 SINUMERIK 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 two comfortable methods is provided.

5.2 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.

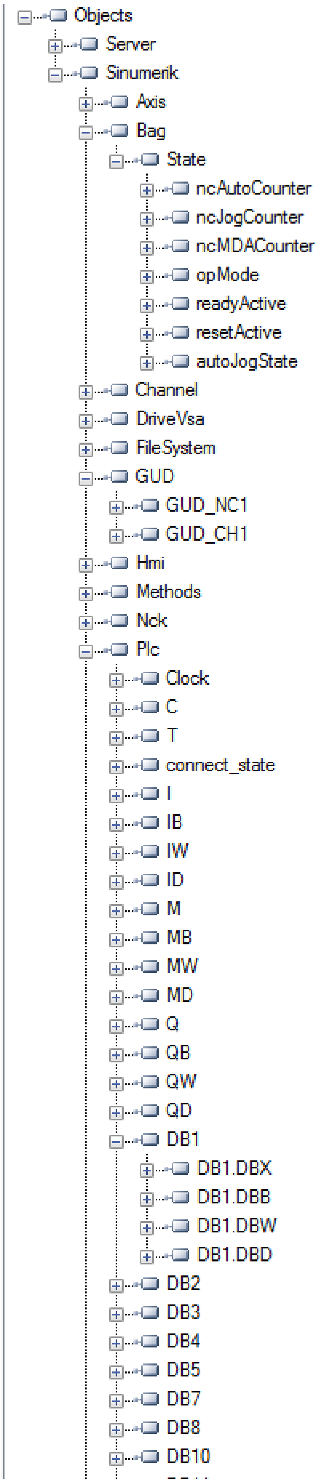
The PLC blocks (inputs, outputs, bit memory, data blocks) can be found under the "/Sinumerik/Plc" node.

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.



```
Objects
  Server
  Sinumerik
    Axis
    Bag
      State
        ncAutoCounter
        ncJogCounter
        ncMDACounter
        opMode
        readyActive
        resetActive
        autoJogState
    Channel
    DriveVsa
    FileSystem
    GUD
      GUD_NC1
      GUD_CH1
    Hmi
    Methods
    Nck
    Plc
      Clock
      C
      T
      connect_state
      I
      IB
      IW
      ID
      M
      MB
      MW
      MD
      Q
      QB
      QW
      QD
      DB1
        DB1.DBX
        DB1.DBB
        DB1.DBW
        DB1.DBD
      DB2
      DB3
      DB4
      DB5
      DB7
      DB8
      DB10
```

Figure 5-1 Browsing

5.3 Variable access

5.3.1 Variable paths for NC access operations

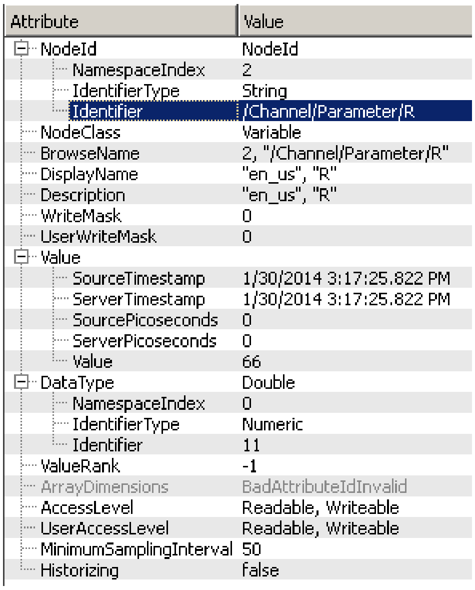
Note

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 additional information from the List Manual for 840D sl and 828D "NC variables and interface signals" (https://support.industry.siemens.com/cs/de/de/view/109748365/en).



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 5-2 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 5-1 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]).

5.3.2 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]
```

5.3.3 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 5-2 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 5-3 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.

5.3.4 Variable paths for machine and setting data

The variable paths for machine and setting data are stored in the address space of the SINUMERIK Operate 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 5-4 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.

5.3.5 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 SINUMERIK 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

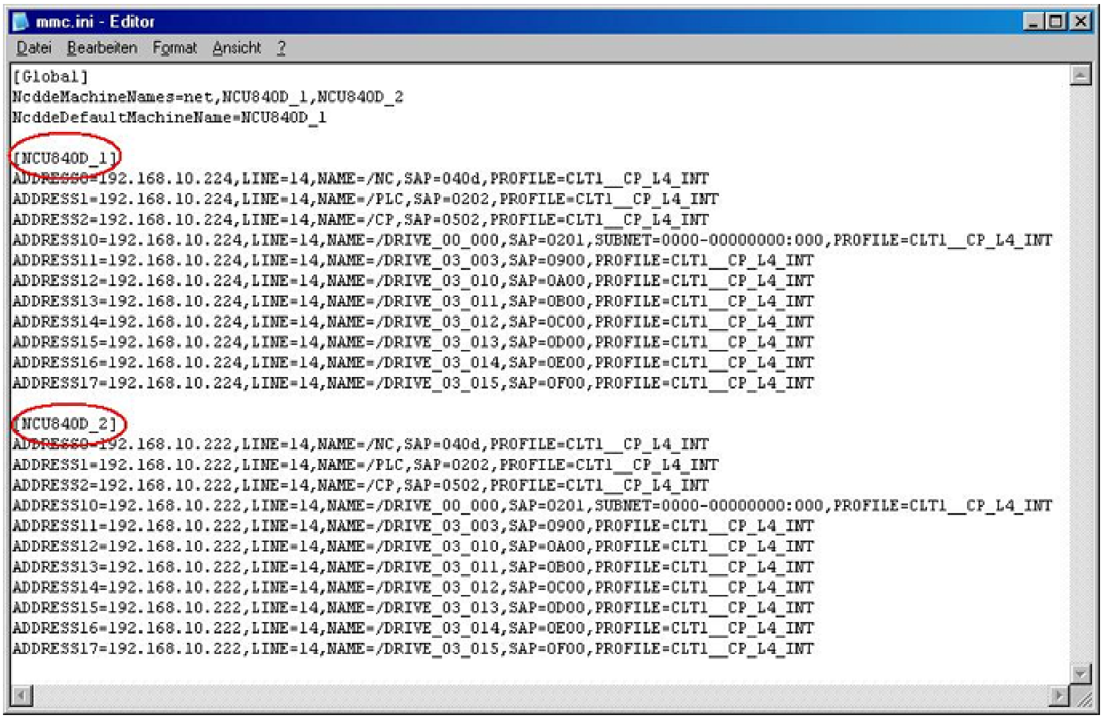
Note

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

Entry:

[GLOBAL]

NcddeMachineNames=NCU1,NCU2



```
[Global]
NcddeMachineNames=net,NCU840D_1,NCU840D_2
NcddeDefaultMachineName=NCU840D_1

[NCU840D_1]
ADDRESS0=192.168.10.224,LINE=14,NAME=/NC,SAP=040d,PROFILE=CLT1__CP_L4_INT
ADDRESS1=192.168.10.224,LINE=14,NAME=/PLC,SAP=0202,PROFILE=CLT1__CP_L4_INT
ADDRESS2=192.168.10.224,LINE=14,NAME=/CP,SAP=0502,PROFILE=CLT1__CP_L4_INT
ADDRESS10=192.168.10.224,LINE=14,NAME=/DRIVE_00_000,SAP=0201,SUBNET=0000-00000000:000,PROFILE=CLT1__CP_L4_INT
ADDRESS11=192.168.10.224,LINE=14,NAME=/DRIVE_03_003,SAP=0900,PROFILE=CLT1__CP_L4_INT
ADDRESS12=192.168.10.224,LINE=14,NAME=/DRIVE_03_010,SAP=0A00,PROFILE=CLT1__CP_L4_INT
ADDRESS13=192.168.10.224,LINE=14,NAME=/DRIVE_03_011,SAP=0B00,PROFILE=CLT1__CP_L4_INT
ADDRESS14=192.168.10.224,LINE=14,NAME=/DRIVE_03_012,SAP=0C00,PROFILE=CLT1__CP_L4_INT
ADDRESS15=192.168.10.224,LINE=14,NAME=/DRIVE_03_013,SAP=0D00,PROFILE=CLT1__CP_L4_INT
ADDRESS16=192.168.10.224,LINE=14,NAME=/DRIVE_03_014,SAP=0E00,PROFILE=CLT1__CP_L4_INT
ADDRESS17=192.168.10.224,LINE=14,NAME=/DRIVE_03_015,SAP=0F00,PROFILE=CLT1__CP_L4_INT

[NCU840D_2]
ADDRESS0=192.168.10.222,LINE=14,NAME=/NC,SAP=040d,PROFILE=CLT1__CP_L4_INT
ADDRESS1=192.168.10.222,LINE=14,NAME=/PLC,SAP=0202,PROFILE=CLT1__CP_L4_INT
ADDRESS2=192.168.10.222,LINE=14,NAME=/CP,SAP=0502,PROFILE=CLT1__CP_L4_INT
ADDRESS10=192.168.10.222,LINE=14,NAME=/DRIVE_00_000,SAP=0201,SUBNET=0000-00000000:000,PROFILE=CLT1__CP_L4_INT
ADDRESS11=192.168.10.222,LINE=14,NAME=/DRIVE_03_003,SAP=0900,PROFILE=CLT1__CP_L4_INT
ADDRESS12=192.168.10.222,LINE=14,NAME=/DRIVE_03_010,SAP=0A00,PROFILE=CLT1__CP_L4_INT
ADDRESS13=192.168.10.222,LINE=14,NAME=/DRIVE_03_011,SAP=0B00,PROFILE=CLT1__CP_L4_INT
ADDRESS14=192.168.10.222,LINE=14,NAME=/DRIVE_03_012,SAP=0C00,PROFILE=CLT1__CP_L4_INT
ADDRESS15=192.168.10.222,LINE=14,NAME=/DRIVE_03_013,SAP=0D00,PROFILE=CLT1__CP_L4_INT
ADDRESS16=192.168.10.222,LINE=14,NAME=/DRIVE_03_014,SAP=0E00,PROFILE=CLT1__CP_L4_INT
ADDRESS17=192.168.10.222,LINE=14,NAME=/DRIVE_03_015,SAP=0F00,PROFILE=CLT1__CP_L4_INT
```

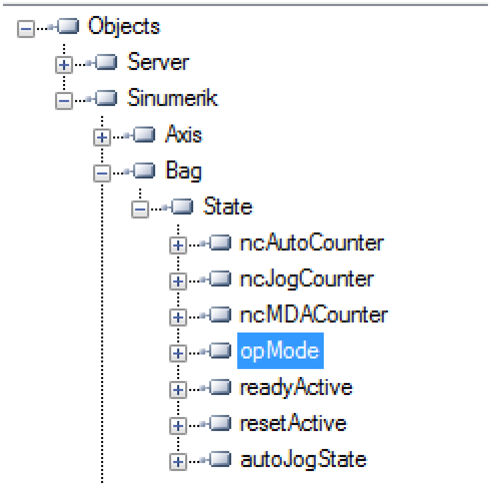
Figure 5-3 NCU names with 1:N

5.3.6 Finding of OPC UA variables

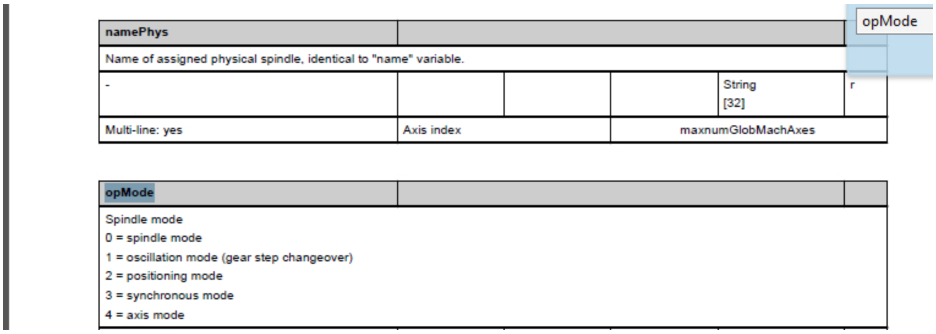
For more information on variable documentation, refer: NC variables and interface signals (https://support.industry.siemens.com/cs/de/de/view/109748365/en)

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".

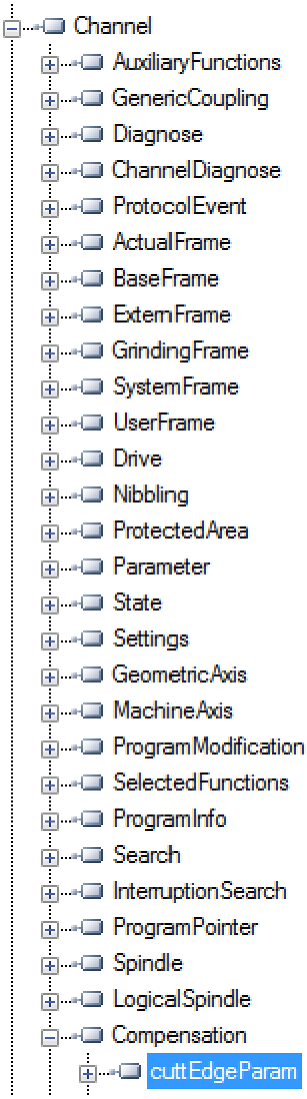


namePhys					
Name of assigned physical spindle, identical to "name" variable.					
-				String [32]	r
Multi-line: yes	Axis index		maxnumGlobMachAxes		

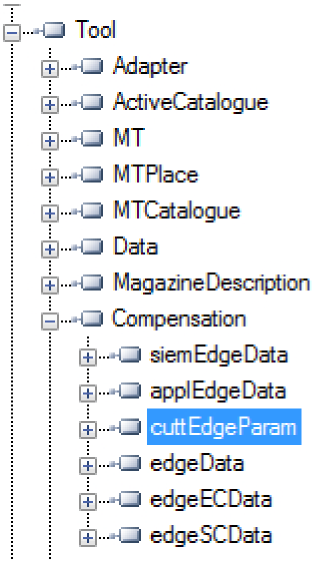
opMode		
Spindle mode 0 = spindle mode 1 = oscillation mode (gear step changeover) 2 = positioning mode 3 = synchronous mode 4 = axis mode		

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".

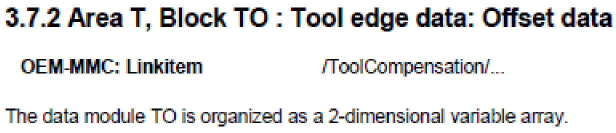


- Channel
  - AuxiliaryFunctions
  - GenericCoupling
  - Diagnose
  - ChannelDiagnose
  - ProtocolEvent
  - ActualFrame
  - BaseFrame
  - ExternFrame
  - GrindingFrame
  - SystemFrame
  - UserFrame
  - Drive
  - Nibbling
  - ProtectedArea
  - Parameter
  - State
  - Settings
  - GeometricAxis
  - MachineAxis
  - ProgramModification
  - SelectedFunctions
  - ProgramInfo
  - Search
  - InterruptionSearch
  - ProgramPointer
  - Spindle
  - LogicalSpindle
  - Compensation
    - cuttEdgeParam



- Tool
  - Adapter
  - ActiveCatalogue
  - MT
  - MTPlace
  - MTCatalogue
  - Data
  - MagazineDescription
  - Compensation
    - siemEdgeData
    - applEdgeData
    - cuttEdgeParam
    - edgeData
    - edgeECData
    - edgeSCData

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

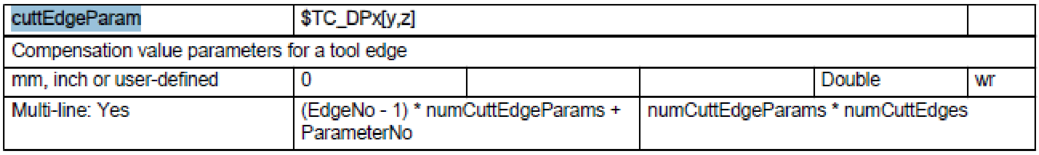


3.7.2 Area T, Block TO : Tool edge data: Offset data

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".

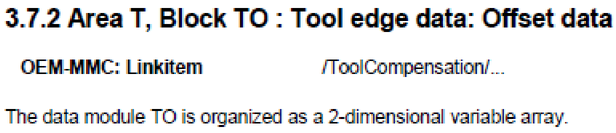


cuttEdgeParam	$TC_DPx[y,z]				
Compensation value parameters for a tool edge					
mm, inch or user-defined	0			Double	wr
Multi-line: Yes	(EdgeNo - 1) * numCuttEdgeParams + ParameterNo		numCuttEdgeParams * numCuttEdges		

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/".

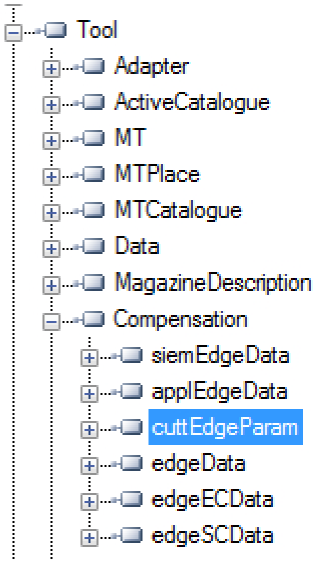


3.7.2 Area T, Block TO : Tool edge data: Offset data

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".



- Tool
  - Adapter
  - ActiveCatalogue
  - MT
  - MTPlace
  - MTCatalogue
  - Data
  - MagazineDescription
  - Compensation
    - siemEdgeData
    - applEdgeData
    - cuttEdgeParam
    - edgeData
    - edgeECData
    - edgeSCData

5.3.7 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 99)

5.4 Alarms

5.4.1 Overview

Any OPC UA client supporting Alarms & Conditions connected to the SINUMERIK 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.

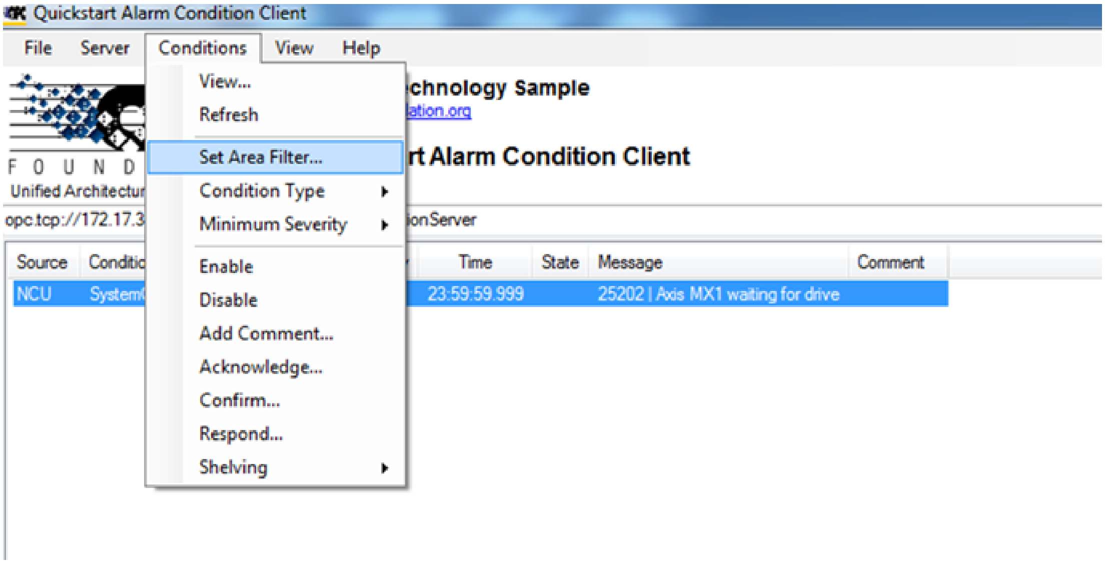
Multi language support for the alarms and warnings messages are supported and the required alarm language can be selected during session creation in OPC UA Client. If the desired language is not supported in the operate, the default English language is supported.
The SINUMERIK Alarm object is of the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

5.4.2 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".



Source	Conditio	Time	State	Message	Comment
NCU	System(	23:59:59.999		25202 | Axis MX1 waiting for drive	

Figure 5-4 Alarm Condition Client

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

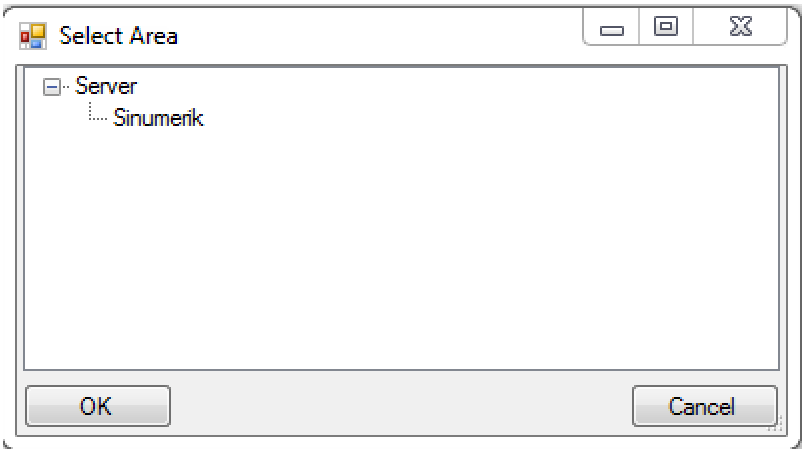
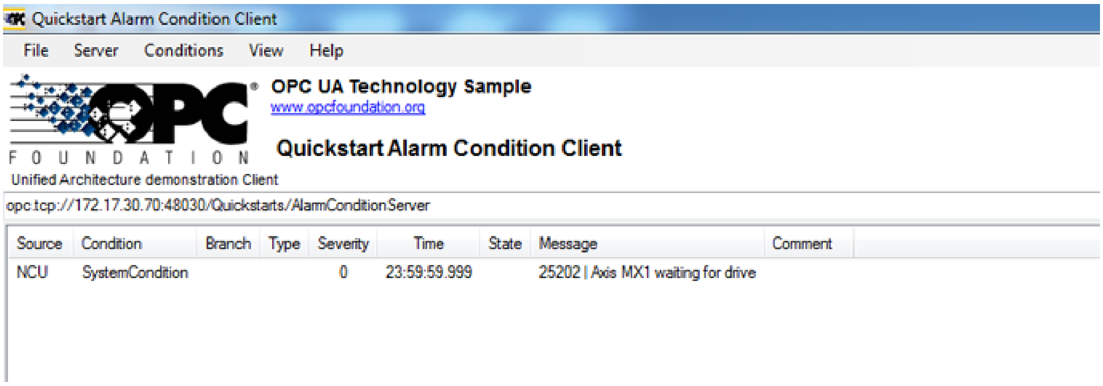


Figure 5-5 The Select Area Window

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

The alarms will be displayed on the screen.


Quickstart Alarm Condition Client
File
Server
Conditions
View
Help
OPC
FOUNDATION
OPC UA Technology Sample
www.opcfoundation.org
Quickstart Alarm Condition Client
Unified Architecture demonstration Client

opc.tcp://172.17.30.70:48030/Quickstarts/AlarmConditionServer

Source	Condition	Branch	Type	Severity	Time	State	Message	Comment
NCU	SystemCondition			0	23:59:59.999		25202 | Axis MX1 waiting for drive	

Figure 5-6 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.

5.4.3 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.

5.4.4 SINUMERIK Alarm object

5.4.4.1 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.

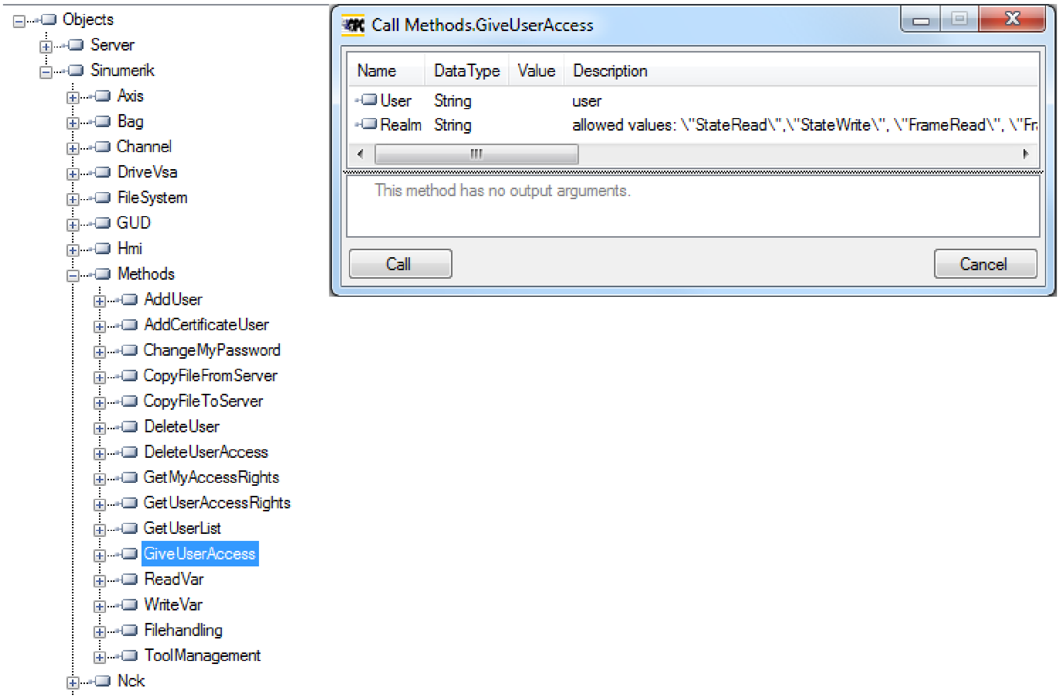
Events are by themselves not visible as nodes in the address space. They can only be received via objects. Not all objects can signal events. Whether an object can signal events is specified at the object by the EventNotifier attribute. Only objects where this attribute has been set can be specified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

5.4.4.2 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.



Name	DataType	Value	Description
User	String		user
Realm	String		allowed values: \"StateRead\",\"StateWrite\", \"FrameRead\", \"Fr

This method has no output arguments.

Figure 5-7 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.

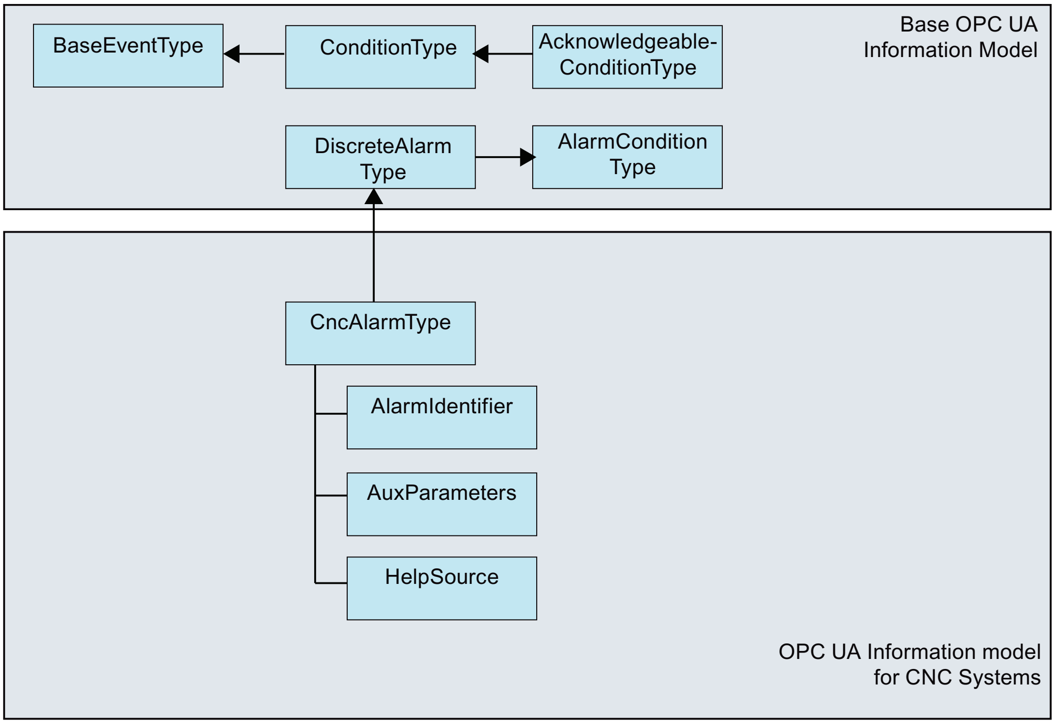


Figure 5-8 OPC UA Information Model for CNC Systems

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.

Attribute	Data type	Mapping with respect to SINUMERIK	M/O	Description
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.

Attribute	Data type	Mapping with respect to SINUMERIK	M/O	Description

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.
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

Attribute	Data type	Mapping with respect to SINUMERIK	M/O	Description
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.

5.4.5 Language of alarms

5.4.5.1 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

For more information, refer to the specification **OPC UA Part3 - Address Space Model 1.03 Specification.pdf**

5.4.5.2 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.

5.4.5.3 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
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

Language	SINUMERIK LanguageID	OPC UA Specific LocaleId
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.

5.4.6 OPC UA alarms and conditions constraints

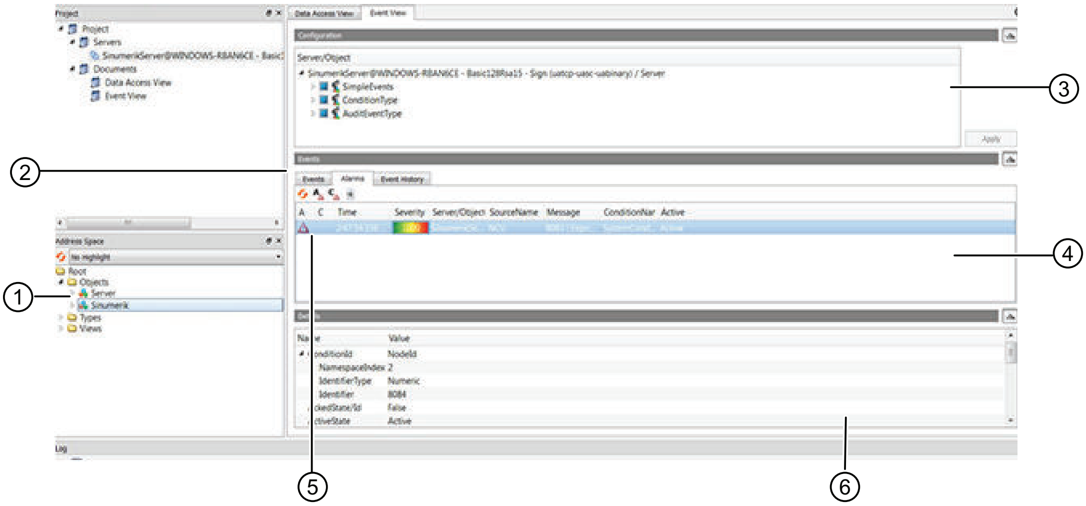
Below are the features which are not supported in this version:

- 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.

5.4.7 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.



Name	Value
onditionId	NodeId
NamespaceIndex	2
IdentifierType	Numeric
Identifier	8084
ckedState/Id	False
ctiveState	Active

① Alarm / Event Instances:
The user needs to subscribe to these instances (by dragging or by configuring).

② The Alarm / Event Subscription View

③ The Alarm window

④ 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

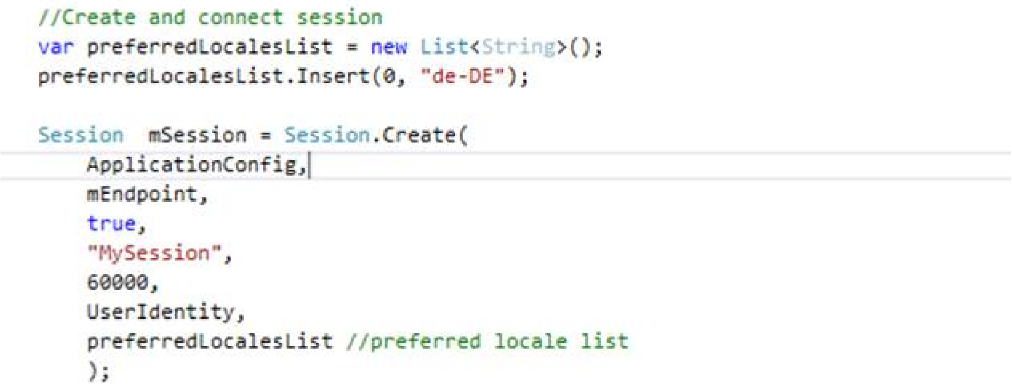
⑤ In the first column of the Alarm tab, a symbol indicates whether an event has already been Acknowledged. (red flag: unacknowledged, green checkmark: acknowledged)

⑥ For the currently selected event in the events list (4) all events fields are displayed which were supplied for this event.

Figure 5-9 User interface UaExpert client

5.4.8 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.

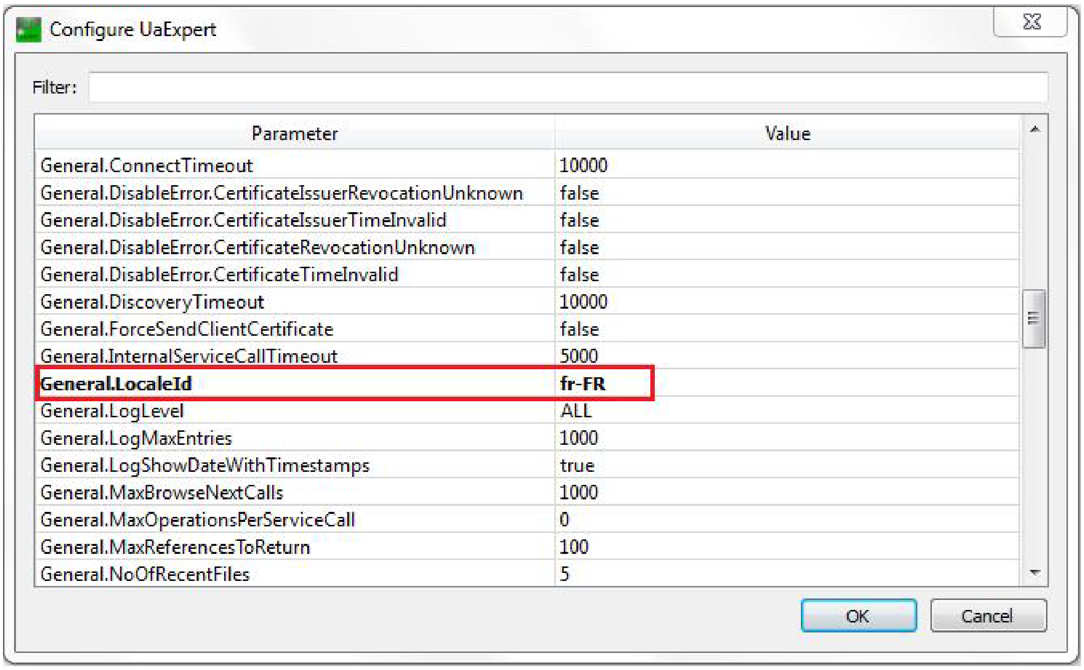


```
//Create and connect session
var preferredLocalesList = new List<String>();
preferredLocalesList.Insert(0, "de-DE");

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

Figure 5-10 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.



Parameter	Value
General.ConnectTimeout	10000
General.DisableError.CertificateIssuerRevocationUnknown	false
General.DisableError.CertificateIssuerTimeInvalid	false
General.DisableError.CertificateRevocationUnknown	false
General.DisableError.CertificateTimeInvalid	false
General.DiscoveryTimeout	10000
General.ForceSendClientCertificate	false
General.InternalServiceCallTimeout	5000
General.LocaleId	**fr-FR**
General.LogLevel	ALL
General.LogMaxEntries	1000
General.LogShowDateWithTimestamps	true
General.MaxBrowseNextCalls	1000
General.MaxOperationsPerServiceCall	0
General.MaxReferencesToReturn	100
General.NoOfRecentFiles	5

Figure 5-11 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

5.5 File system

5.5.1 Overview

The SINUMERIK OPC UA server offers two methods to copy NC part program from OPC UA client to the SINUMERIK server and vice versa.

Furthermore, the standard OPC UA file and folder objects are supported.

Operations

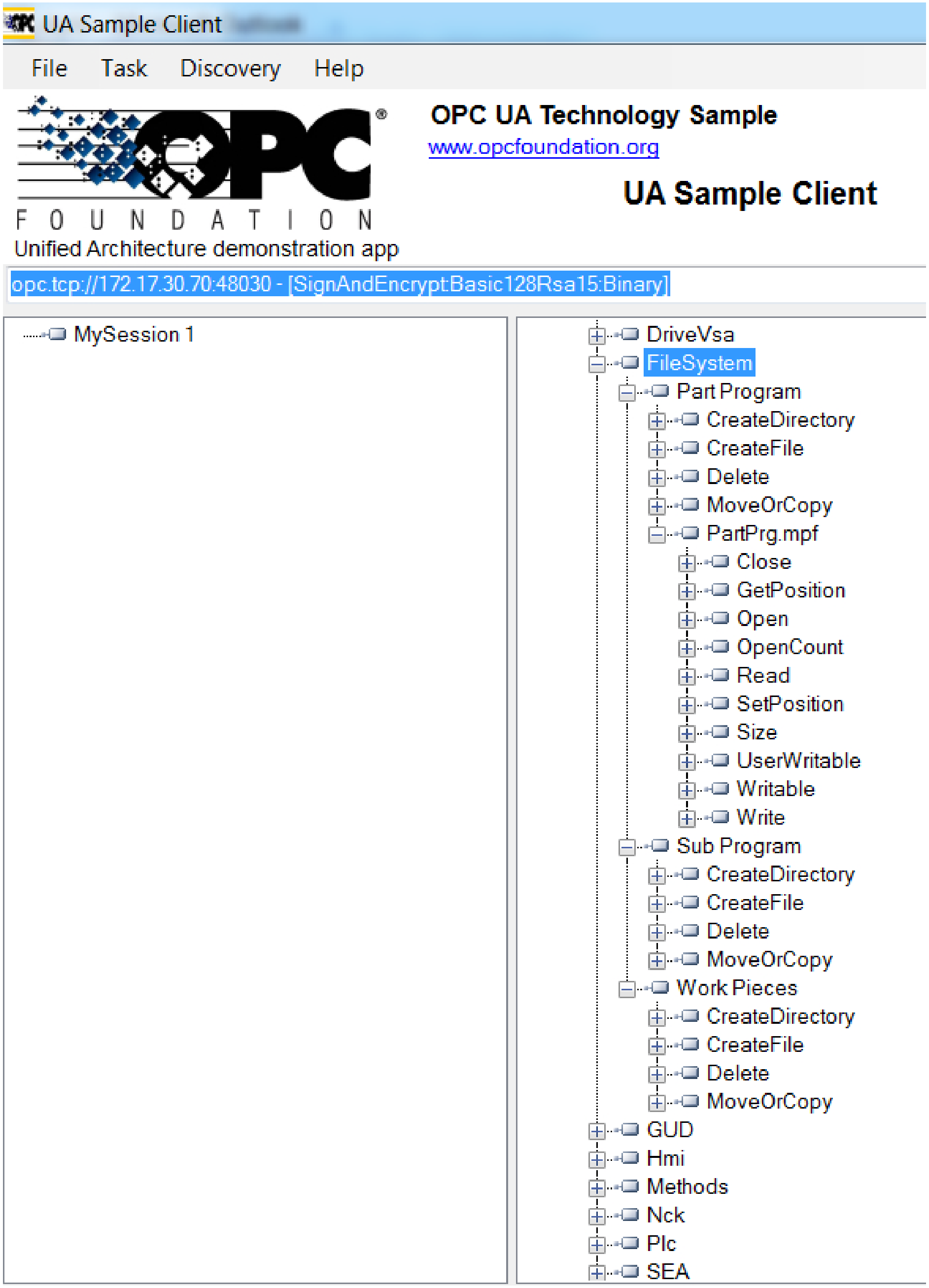
This allows an OPC UA client to use the following operations within the part of the SINUMERIK file system:

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



- DriveVsa
- FileSystem
  - Part Program
    - CreateDirectory
    - CreateFile
    - Delete
    - MoveOrCopy
    - PartPrg.mpf
      - Close
      - GetPosition
      - Open
      - OpenCount
      - Read
      - SetPosition
      - Size
      - UserWritable
      - Writable
      - Write
  - Sub Program
    - CreateDirectory
    - CreateFile
    - Delete
    - MoveOrCopy
  - Work Pieces
    - CreateDirectory
    - CreateFile
    - Delete
    - MoveOrCopy
- GUD
- Hmi
- Methods
- Nck
- Plc
- SEA

Figure 5-12 The file system

5.5.2 File access rights

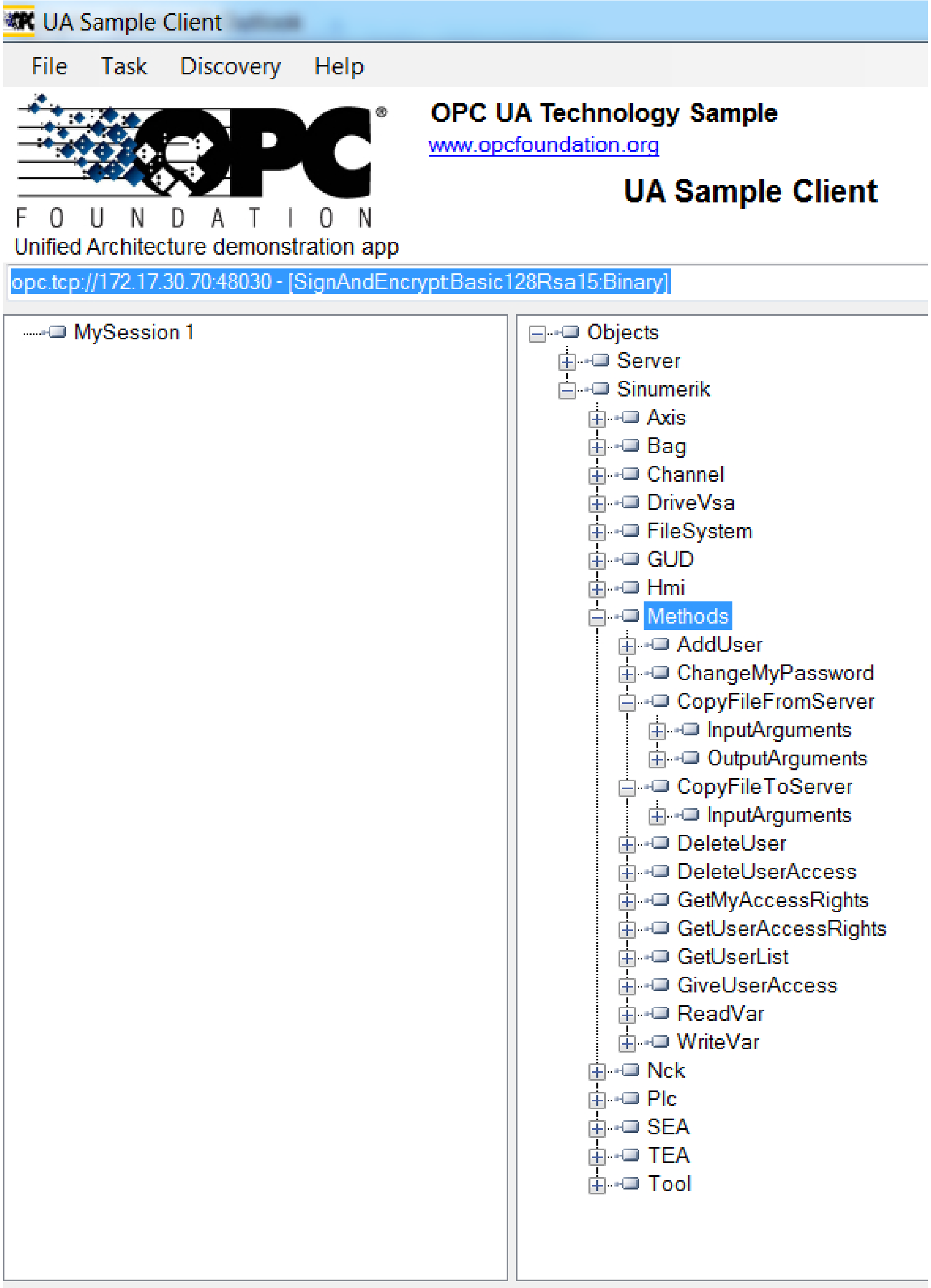
The OPC UA server allows the OPC UA client to support the transfer of files between the client and the server.

The two methods CopyFileToServer and CopyFileFromServer and also standard file system methods need the following access rights:

- FsRead
- FsWrite

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 42)):

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



UA Sample Client [redacted]

File Task Discovery Help

OPC UA Technology Sample
www.opcfoundation.org

UA Sample Client

FOUNDATION
Unified Architecture demonstration app

opc.tcp://172.17.30.70:48030 - [SignAndEncrypt:Basic128Rsa15:Binary]

```
MySession 1
```

```
Objects
  Server
  Sinumerik
    Axis
    Bag
    Channel
    DriveVsa
    FileSystem
    GUD
    Hmi
    Methods
      AddUser
      ChangeMyPassword
      CopyFileFromServer
        InputArguments
        OutputArguments
      CopyFileToServer
        InputArguments
      DeleteUser
      DeleteUserAccess
      GetMyAccessRights
      GetUserAccessRights
      GetUserList
      GiveUserAccess
      ReadVar
      WriteVar
    Nck
    Plc
    SEA
    TEA
    Tool
```

Figure 5-13 Standard Method

5.5.3 Standard file system support

Standard methods for File Transfer

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. The folders, "Part Programs", "Sub Programs" and "Work Pieces" are of the "FolderType" type, 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.

Here, the files are available with the extensions .mpf, .spf and .wpf respectively under Part Program, Sub Programs and Work Pieces folders of SINUMERIK. Each of these files will be of "FileType" type and consists of 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 the user creates 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 Typedefinition in the OPC UA Specification Part 5.

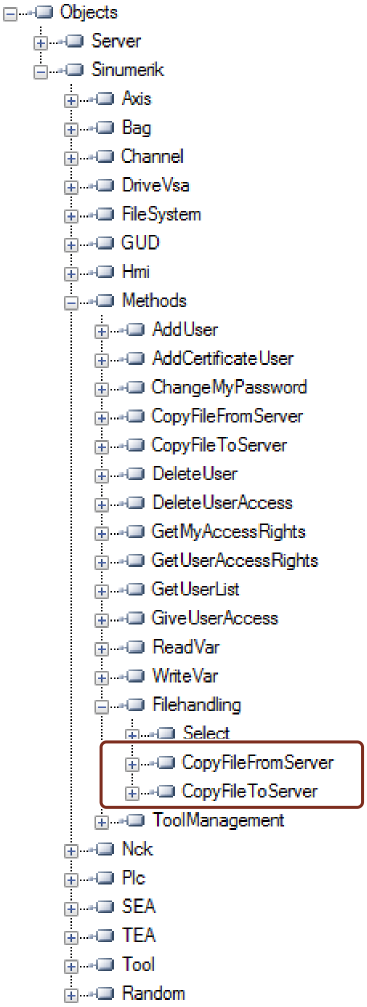
Note

No multiple extensions supported

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

Methods supported for File Transfer

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



- Objects
  - Server
  - Sinumerik
    - Axis
    - Bag
    - Channel
    - DriveVsa
    - FileSystem
    - GUD
    - Hmi
    - Methods
      - AddUser
      - AddCertificateUser
      - ChangeMyPassword
      - CopyFileFromServer
      - CopyFileToServer
      - DeleteUser
      - DeleteUserAccess
      - GetMyAccessRights
      - GetUserAccessRights
      - GetUserList
      - GiveUserAccess
      - ReadVar
      - WriteVar
      - Filehandling
        - Select
        - CopyFileFromServer
        - CopyFileToServer
      - ToolManagement
    - Nck
    - Plc
    - SEA
    - TEA
    - Tool
    - Random

Figure 5-14 Methods for the file transfer

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.

Out of security reasons only the following folders are accessible:

- Part Programs
- Sub Programs
- Work Pieces.

For example:

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

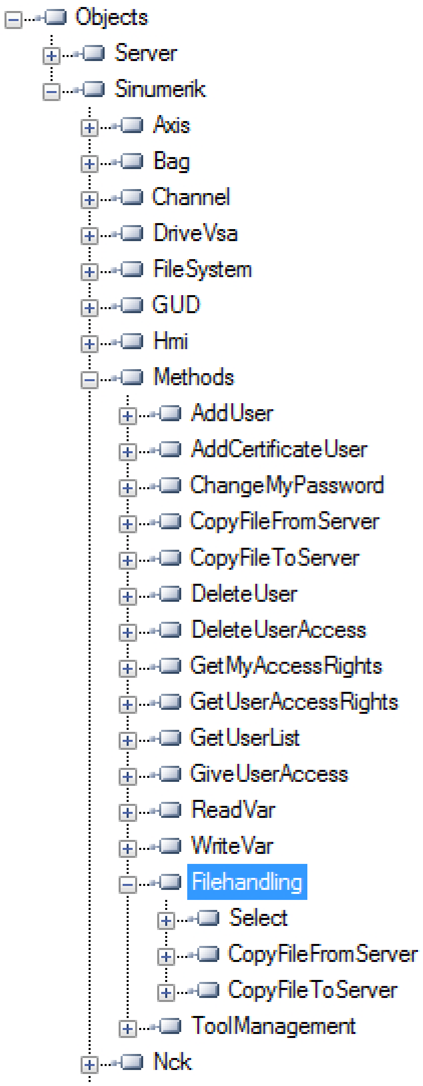
- Sinumerik/FileSystem/Part Program/partprg.mpf
- Sinumerik/FileSystem/Sub Program/subprg.spf
- Sinumerik/FileSystem/Work Pieces/wrkprg.wpf

5.6 Select

5.6.1 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.



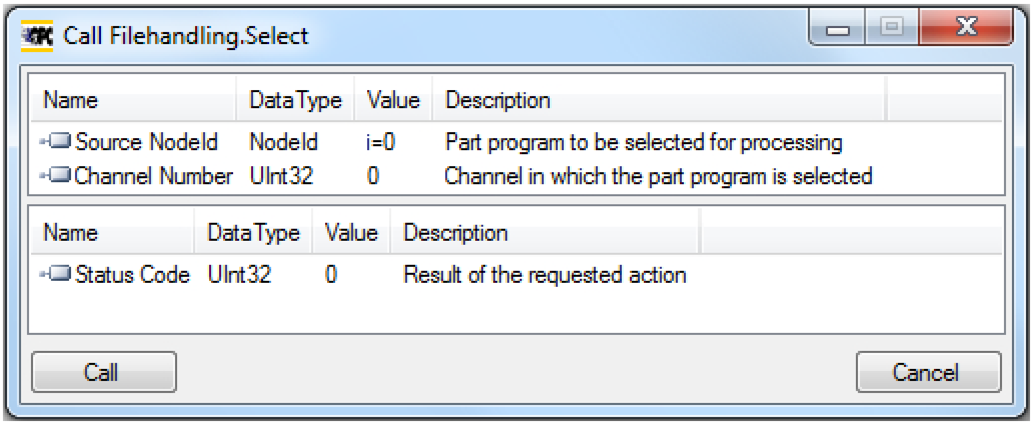
5.6.2 Description

You are allowed to select the part program file for execution from the NC file system. 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.



Name	Data Type	Value	Description
Source NodeId	NodeId	i=0	Part program to be selected for processing
Channel Number	UInt32	0	Channel in which the part program is selected

Name	Data Type	Value	Description
Status Code	UInt32	0	Result of the requested action

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

5.6.3 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

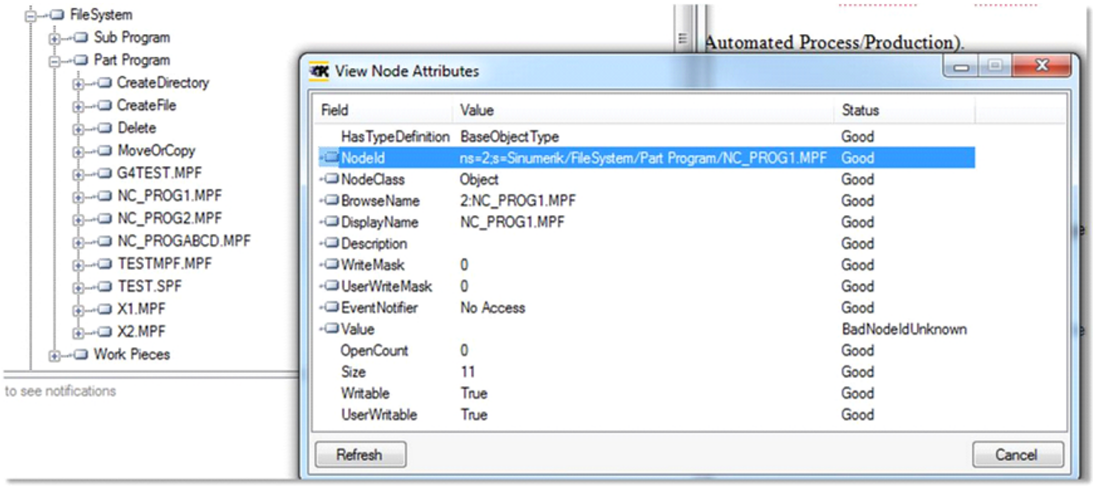
The following table gives details on values and description of the OPC UA method call status:

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.

5.6.4 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.



- FileSystem
  - Sub Program
  - Part Program
    - CreateDirectory
    - CreateFile
    - Delete
    - MoveOrCopy
    - G4TEST.MPF
    - NC_PROG1.MPF
    - NC_PROG2.MPF
    - NC_PROGABCD.MPF
    - TESTMPF.MPF
    - TEST.SPF
    - X1.MPF
    - X2.MPF
  - Work Pieces

to see notifications

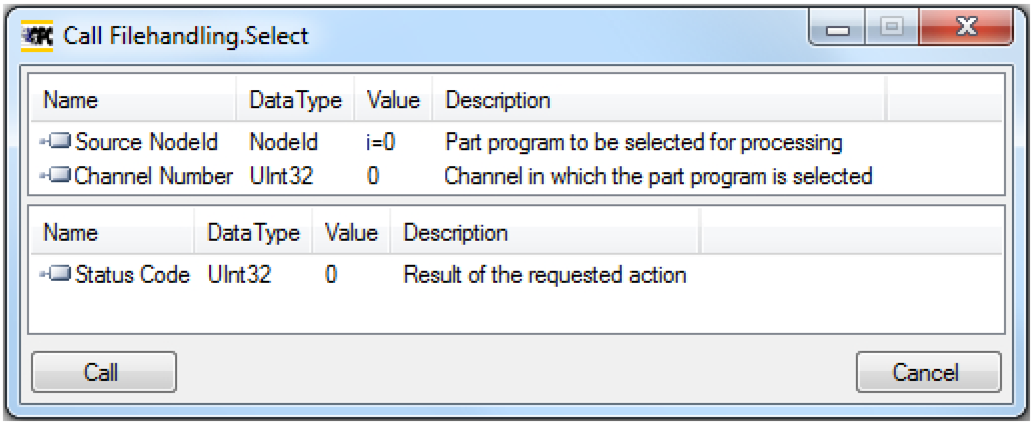
Automated Process/Production).

View Node Attributes

Field	Value	Status
HasTypeDefinition	BaseObjectType	Good
NodeId	ns=2;s=Sinumerik/FileSystem/Part Program/NC_PROG1.MPF	Good
NodeClass	Object	Good
BrowseName	2:NC_PROG1.MPF	Good
DisplayName	NC_PROG1.MPF	Good
Description		Good
WriteMask	0	Good
UserWriteMask	0	Good
EventNotifier	No Access	Good
Value		BadNodeIdUnknown
OpenCount	0	Good
Size	11	Good
Writable	True	Good
UserWritable	True	Good

Figure 5-15 Finding of NodeID

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



Call Filehandling.Select

Name	DataType	Value	Description
Source NodeId	NodeId	i=0	Part program to be selected for processing
Channel Number	UInt32	0	Channel in which the part program is selected

Name	DataType	Value	Description
Status Code	UInt32	0	Result of the requested action

Figure 5-16 Arguments of select method

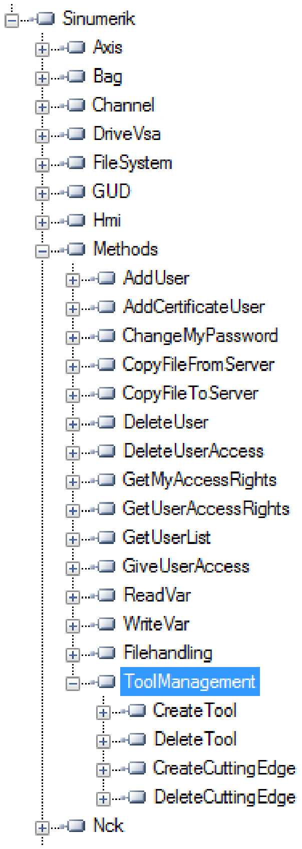
The particular part program will be selected.

5.7 Tool management

5.7.1 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



- Sinumerik
  - Axis
  - Bag
  - Channel
  - DriveVsa
  - FileSystem
  - GUD
  - Hmi
  - Methods
    - AddUser
    - AddCertificateUser
    - ChangeMyPassword
    - CopyFileFromServer
    - CopyFileToServer
    - DeleteUser
    - DeleteUserAccess
    - GetMyAccessRights
    - GetUserAccessRights
    - GetUserList
    - GiveUserAccess
    - ReadVar
    - WriteVar
    - Filehandling
    - ToolManagement
      - CreateTool
      - DeleteTool
      - CreateCuttingEdge
      - DeleteCuttingEdge
  - Nck

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

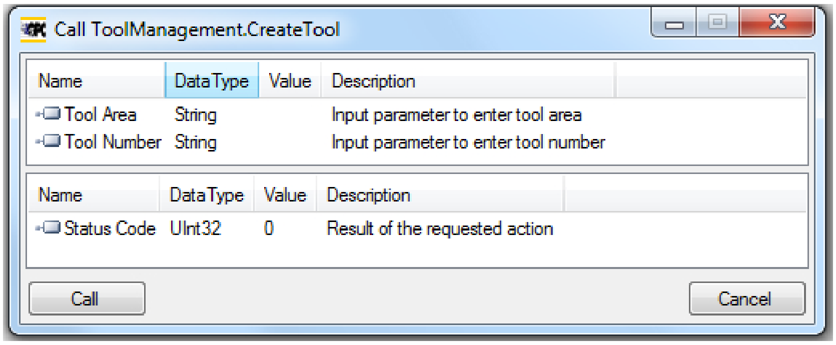
The access right for the user is provided using the "GiveUserAccess" method.

5.7.2 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
)
```



Call ToolManagement.CreateTool

Name	Data Type	Value	Description
Tool Area	String		Input parameter to enter tool area
Tool Number	String		Input parameter to enter tool number

Name	Data Type	Value	Description
Status Code	UInt32	0	Result of the requested action

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

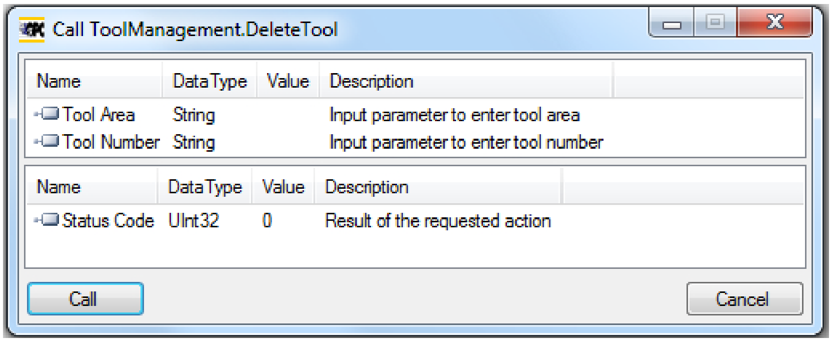
Result	Description
Succeeded	Method executed with success/failure reason.
BadInvalidArgument	Arguments provided are not correct.
BadUserAccessDenied	"ToolWrite" access is not provided.

5.7.3 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
)
```



Call ToolManagement.DeleteTool

Name	DataType	Value	Description
Tool Area	String		Input parameter to enter tool area
Tool Number	String		Input parameter to enter tool number

Name	DataType	Value	Description
Status Code	UInt32	0	Result of the requested action

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.

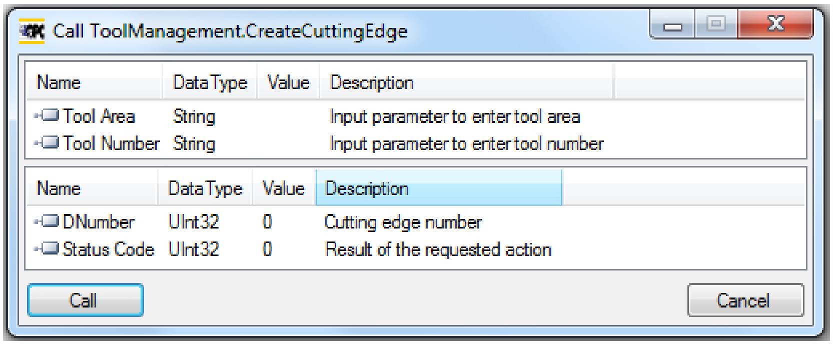
5.7.4 CreateCuttingEdge

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
)
```



Call ToolManagement.CreateCuttingEdge

Name	Data Type	Value	Description
Tool Area	String		Input parameter to enter tool area
Tool Number	String		Input parameter to enter tool number

Name	Data Type	Value	Description
DNumber	UInt32	0	Cutting edge number
Status Code	UInt32	0	Result of the requested action

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.

5.7.5 DeleteCuttingEdge

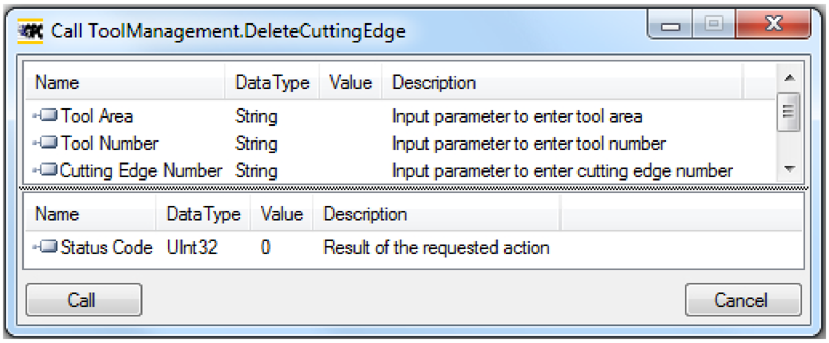
The "DeleteCuttingEdge" is used to delete a cutting edge of an existing tool in "Tool List" section of the SINUMERIK. This method appears under the folder "Methods/ToolManagement".

The DeleteCuttingEdge method has three input and one output parameters.

`Signature`:

```
DeleteCuttingEdge(

[in] string ToolArea

[in] string ToolNumber

[in] string CuttingEdgeNumber

[out] Uint32 StatusCode
```

)



Name	DataType	Value	Description
Tool Area	String		Input parameter to enter tool area
Tool Number	String		Input parameter to enter tool number
Cutting Edge Number	String		Input parameter to enter cutting edge number

Name	DataType	Value	Description
Status Code	UInt32	0	Result of the requested action

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.

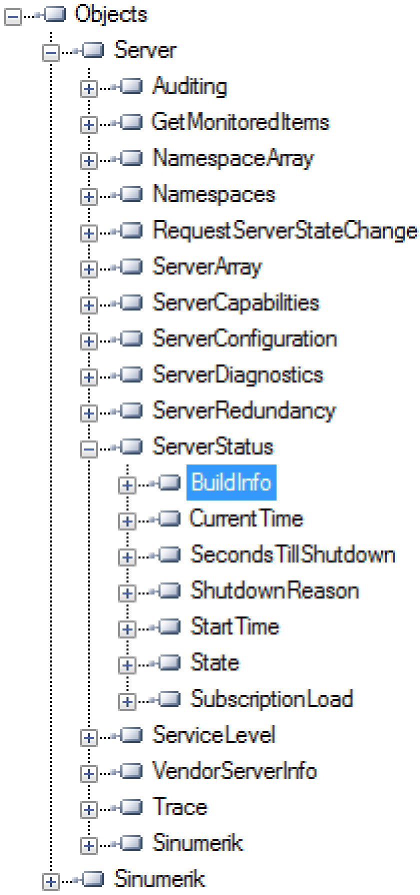
Diagnostics 6

6.1 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:



- Objects
  - Server
    - Auditing
    - GetMonitoredItems
    - NamespaceArray
    - Namespaces
    - RequestServerStateChange
    - ServerArray
    - ServerCapabilities
    - ServerConfiguration
    - ServerDiagnostics
    - ServerRedundancy
    - ServerStatus
      - BuildInfo
      - CurrentTime
      - SecondsTillShutdown
      - ShutdownReason
      - StartTime
      - State
      - SubscriptionLoad
    - ServiceLevel
    - VendorServerInfo
    - Trace
    - Sinumerik
  - Sinumerik

Figure 6-1 Diagnostics Information - Server Node

6.2 Diagnostics screen

Requirement

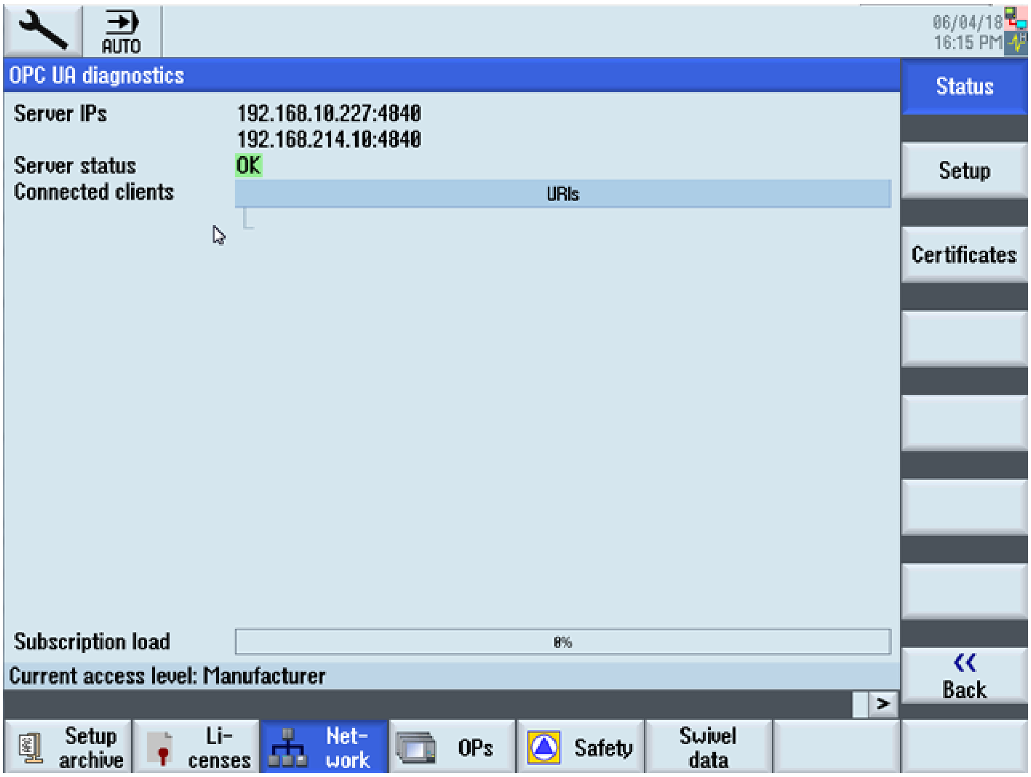
Note

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.

Diagnostics screen

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

To open the diagnostics 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.



OPC UA diagnostics

Server IPs 192.168.10.227:4840
192.168.214.10:4840

Server status OK

Connected clients

URIs

Subscription load 0%

Current access level: Manufacturer

Figure 6-2 Diagnostics

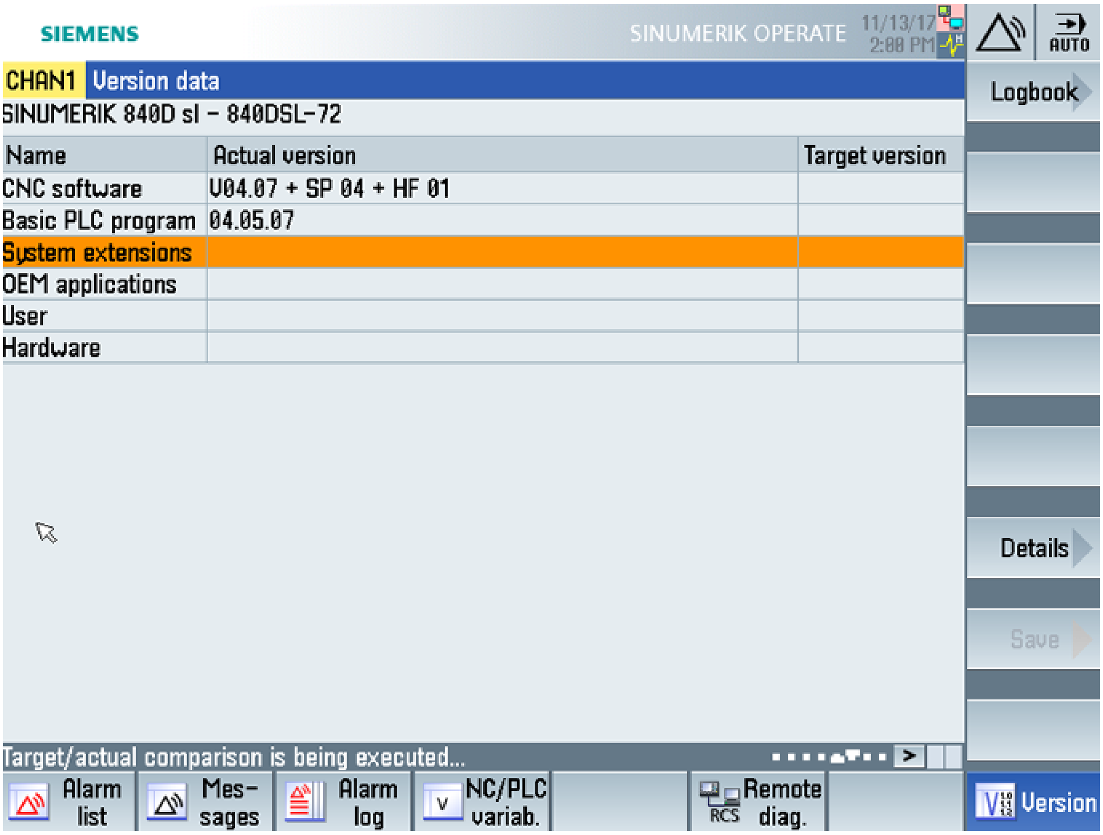
Value	Description	Further explanation
Server IPs	Server IPs and ports of the company network, systems network or service network where the OPC UA server is accessible	
Server status	Possible status of the server: • Ok (server up and running) • Not activated (OPC UA server deactivated) • No connection possible (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, 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 99)), not the overall load.	

6.3 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".



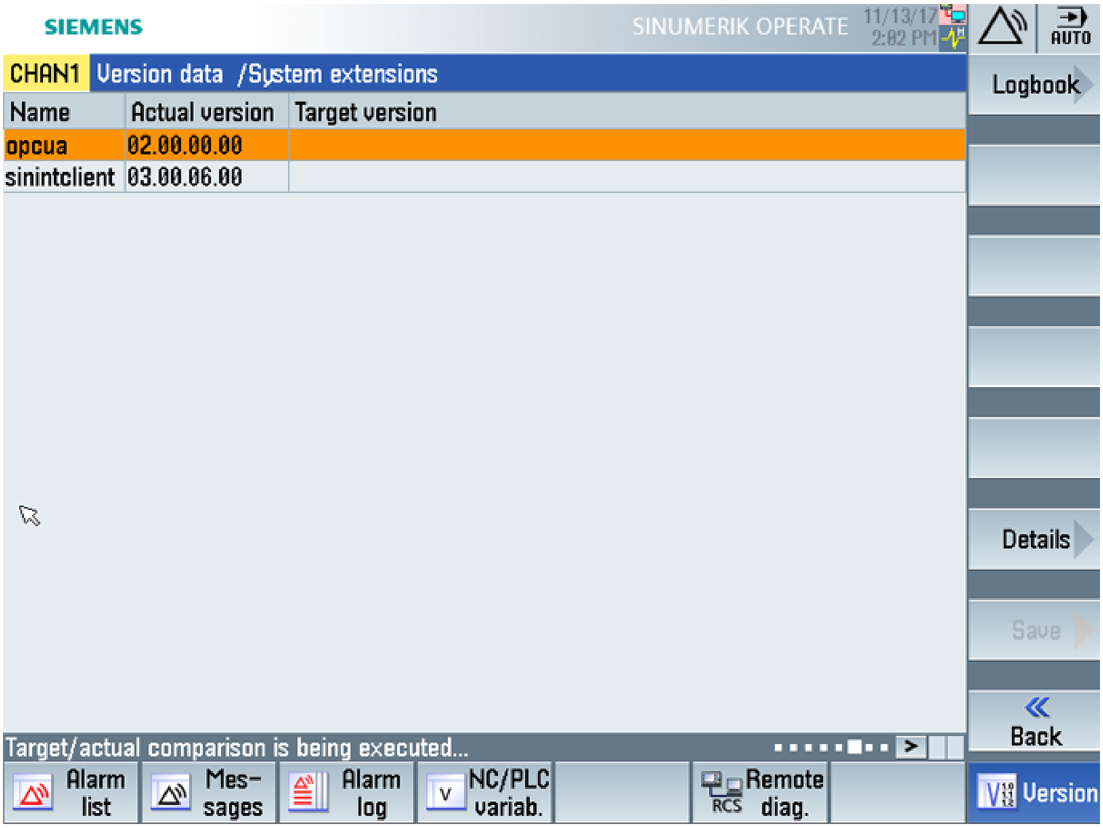
Version data

SINUMERIK 840D sl - 840DSL-72

Name	Actual version	Target version
CNC software	V04.07 + SP 04 + HF 01	
Basic PLC program	04.05.07	
System extensions		
OEM applications		
User		
Hardware		

Target/actual comparison is being executed...

Figure 6-3 Version data



Name	Actual version	Target version
opcua	02.00.00.00	
sinintclient	03.00.06.00	

Target/actual comparison is being executed...

Figure 6-4 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

7

7.1 Overview

Compatibility

This version of OPC UA server is supported by SINUMERIK 840D sl and SINUMERIK 828D. An update process is possible with SINUMERIK software version ≥ V4.7.

SINUMERIK Create MyConfig (CMC)

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

7.2 Installation of OPC UA server

OPC UA - Server update

The installation procedure of the OPC UA server will vary depending whether a PCU or a PPU/NCU is being used. Below are the instructions for both options:

PCU/IPC

1. Load OPC UA software 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 rights will be preserved.

PPU/NCU

1. Load OPC UA software on a bootable 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 rights will be preserved.

7.3 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/).

Technical data 8

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	828D	500 1/s
	840D sl	1000 1/s
Min. sampling interval	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)	3600000 s	
Session timeout	60 s	
Max. monitored items queue size (Subscription Queue size)	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.

Calculating maximum subscription load

The maximum number of monitored items (Page 55) depends on the update time of the subscriptions. Therefore the max. number of monitored items can be calculated as down below.

The maximum subscription load is calculated from the load imposed to the system by the sample rate of all monitored items from all subscriptions of all active sessions.

Max number of monitored items = Systemload / Updates per second

Updates per second = 1 / Sampling rate (in seconds)

Systemload SINUMERIK 840D sl = 1000 items/s

Systemload SINUMERIK 828D = 500 items/s

Trouble shooting 9

9.1 Frequently asked questions (FAQs)

Topic	Question	Possible solution
Setup dialog is not displayed correctly	The OPC UA setup dialog will not be displayed correctly after installation or not to that extent as described in documentation. What can I do?	Possibly the SINUMERIK operating area "Setup" has already been extended by OEM dialogs (function: slsudialog_oem xml). This may cause incorrect functioning of the OPC UA setup dialog in software versions < 4.8 SP2. ● Please contact your regional SIEMENS office or the technical support (https://support.industry.siemens.com/cs/sc/2090/).
OPC UA client has no connection	In spite of correct commissioning my OPC UA client can't 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 setup dialog ● Switch off PCU/NCU/PPU and on again ● Activate OPC UA again in the setup dialog ● Switch off PCU/NCU/PPU and on again
	The server can't 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 setup dialog. The new addresses will be directly transferred into the setup 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?	● Reboot the control in order to activate all necessary firewall settings (e.g.: port number changed).

9.2 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.

Index