SIEMENS

SINUMERIK

SINUMERIK 840D sl SINUMERIK Integrate for Engineering Access MyMachine / OPC UA

Configuration Manual

Valid for:

OPC UA server	Version 2.0
CNC software	Version 4.8 SP2

12/2017
6FC5397-1DP40-6BA1

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: 6FC5397-1DP40-6BA1
℗ 12/2017 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 Integrate 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

Industry 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 Industry 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 38))
- Transfer of part programs (see chapter File transfer (Page 53))
- Event based provision of SINUMERIK alarms and messages from HMI, NC and PLC (see chapter Alarms (Page 45))

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 with high encryption 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 31)).

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

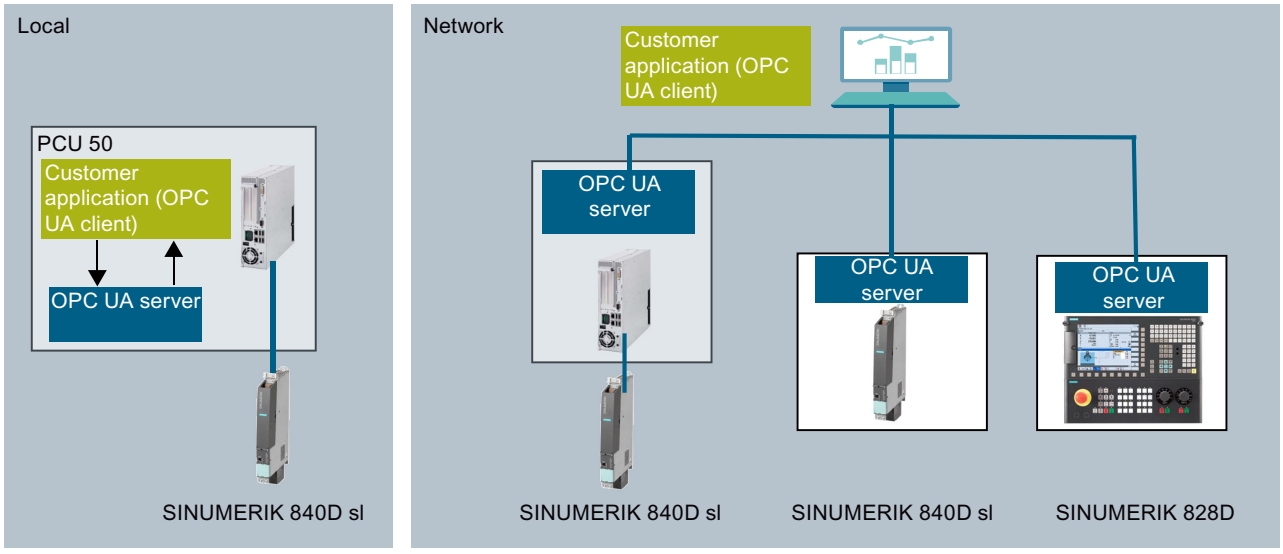


Figure 1-1 Application scenario

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

The application examples are not binding and do not claim to be complete regarding configuration, equipment or any eventuality which may arise. The application examples do not represent specific customer solutions, but are only intended to provide support for typical tasks. You are responsible for the proper operation of the described products. These 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 only represent one component of such a concept.

The customer is responsible for preventing unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit:

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

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

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

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

⚠ 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.

2.2 OPC UA safety notes

NOTICE
Safety risk due to access to security relevant data 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 31), especially chapter List of rights (Page 34).

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).

Requirement

- 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 Licensing

Setting the license

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

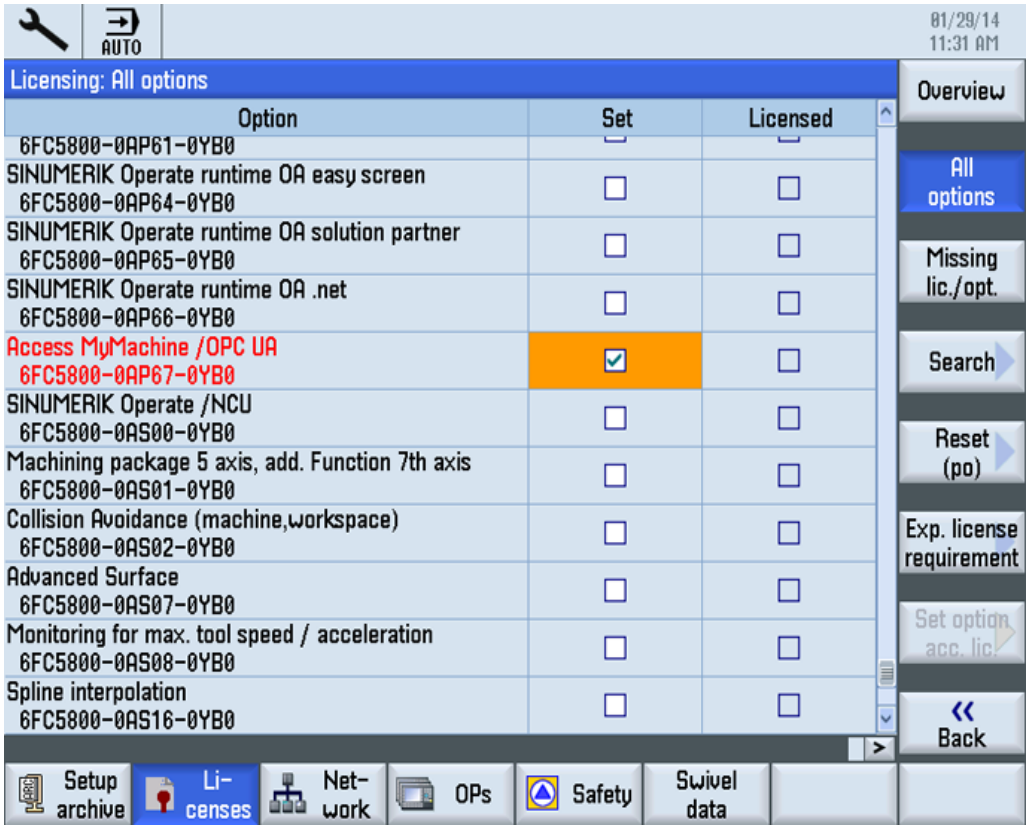


Figure 3-1 Setting the license

2. Restart the SINUMERIK Operate in order to activate the license.

3.3 Commissioning

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.

Note

Please note that the OPC UA softkey is only visible when the license option is set.

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

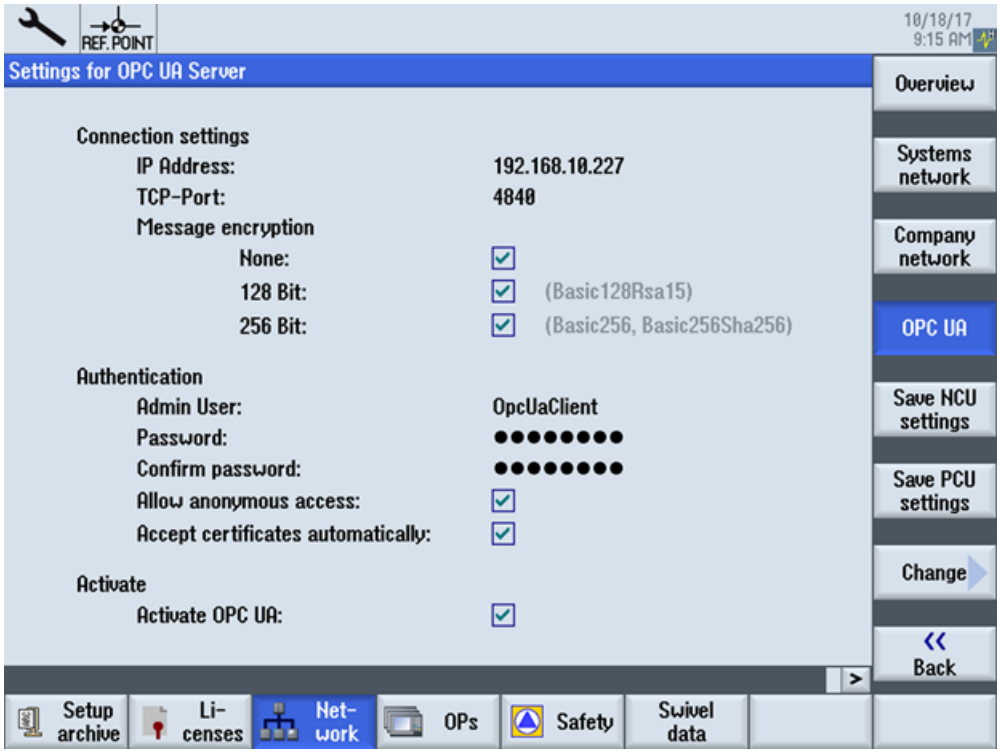


Figure 3-2 Settings of OPC UA Server (with changes)

Group	Setting	Description	
Connection settings	IP address	The IPv4 address of the company network interface, since this is the primary server interface. This is determined automatically. Even if there is only one address stated in this dialog, the OPC UA server is available at the following interfaces:	
		SINUMERIK 828D	-X130
		SINUMERIK 840D sl **without** PCU/IPC	-X120 -X127 -X130
		SINUMERIK 840D sl **with** PCU/IPC	eth1 eth2
		The OPC UA server is always available under the IP address of the network interface where the client interface is connected. **Example for an 840D sl without PCU**: If the client runs on a device, which is connected to X130, the OPC UA server can be addressed using the X130 IP address. On the other hand, if the client is running on a device in the X120 network, then the IP address of the X120 interface must be used.	
	TCP Port	TCP port at which the OPC UA server should be available. Standard configuration: 4840 **Note!** The port must also be open in the firewall. For PPU/NCU this happens automatically. With PCU/IPC the port must be opened manually in the firewall.	
	Message encryption	It can be chosen which security endpoints should be offered from the server	
		Setting	**Standard configuration**
		None	Deactivated
		128 bit	Activated
		256 bit	Activated
Authentication	Admin User	User name of the administrator. The administrator can add or delete users and assign or delete user authorizations.	
	Password	Password of the administrator.	
	Confirm Password	Enter the password again for confirmation.	
	Allow anonymous access	Standard configuration: Deactivated Anonymous access is only recommended for commissioning.	
	Accept certificates automatically	Standard configuration: Activated If this option is set, all client certificates are automatically accepted. For manual acceptance, please refer to chapter Certificate handling (Page 22).	
Activation	Activate OPC UA	Place the checkmark to activate OPC UA and remove the checkmark to deactivate it.	

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 (Page 22)).

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.

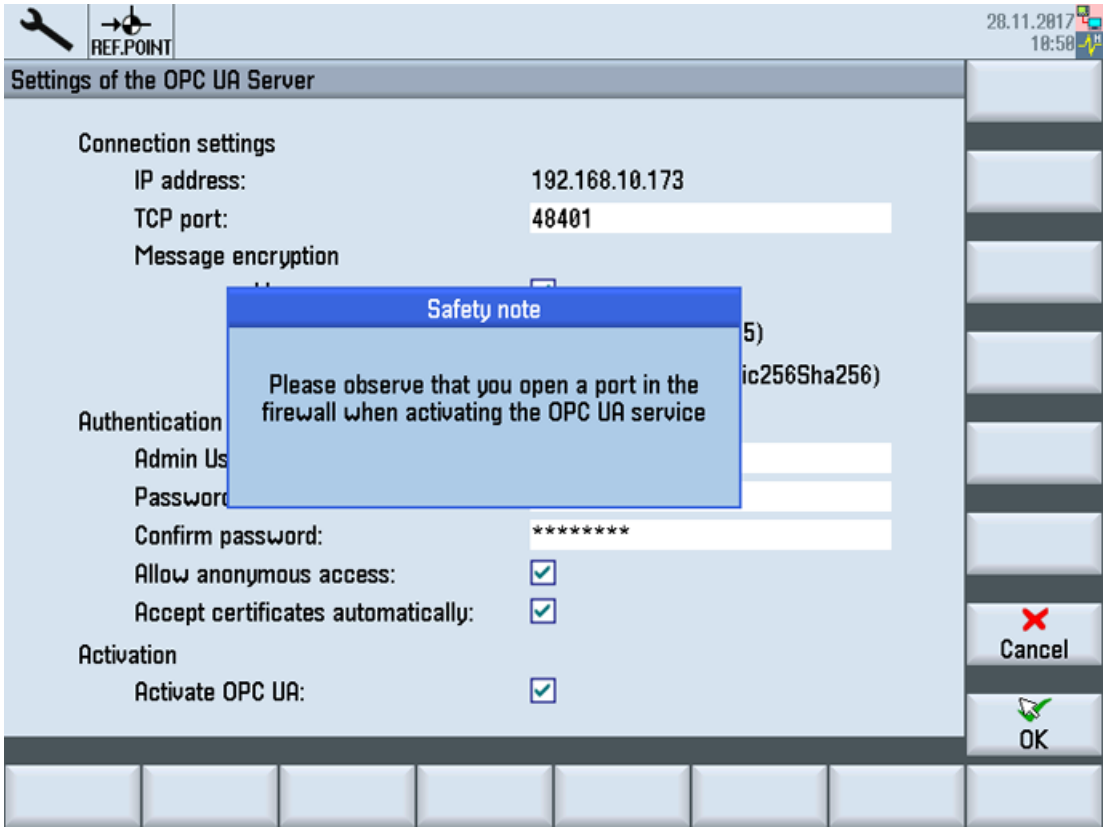


Figure 3-3 Security message for opening the TCP port

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.

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).

3.4 Certificate handling

During the first connection attempt of the client the certificate of the client will be transferred to the SINUMERIK OPC UA server. If the setting "Accept certificates automatically" is set, the client certificate will be automatically trusted and the connection can be established. If the setting is deactivated, the certificate will be treated as untrusted and needs to be trusted manually before the connection can be established.

In this case, the server will report an error (BadSecurityChecksFailed) on initial connection attempt if the provided client certificate is not trusted.

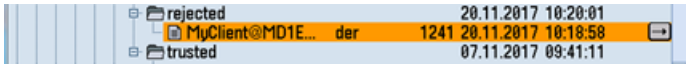
Prerequisites

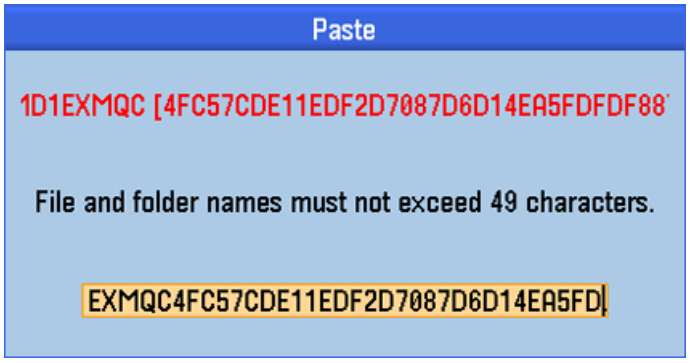
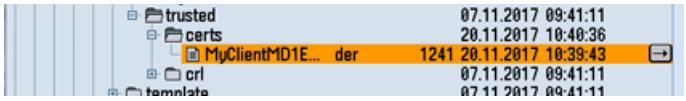
Note

Trusting client certificates is only possible with the SINUMERIK protection level 1 (manufacturer).

Trusting clients certificates manually

This procedure is only necessary, if the setting "Accept certificates automatically" is deactivated.

	1.	Select the operating area "Setup" in SINUMERIK Operate.
	2.	Press the softkey “System data”.
	3.	In the files and folders tree navigate to: • Embedded systems (NCU 840Dsl / 828D): "System CF Card/addon/sinumerik/hmi/opcua/pki/rejected" • PCU system: "System harddisk/C: System/ProgramData/Siemens/MotionControl/addon/sinumerik/hmi/ opcua/pki/rejected"
	4	Select the rejected certificate. 
	5.	Press softkey “Cut”.
	6.	Navigate to folder “trusted/certs”. 
	7.	Press softkey “Paste”.

	8.	The following message will appear: 
	9.	Shorten the filename to match SINUMERIK Operate requirements and make sure the extension (.der) is still appended. Then press softkey “Ok” Verify certificate is in trusted folder: 
	10.	Then the connection to the server can be established from the OPC UA client.

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.

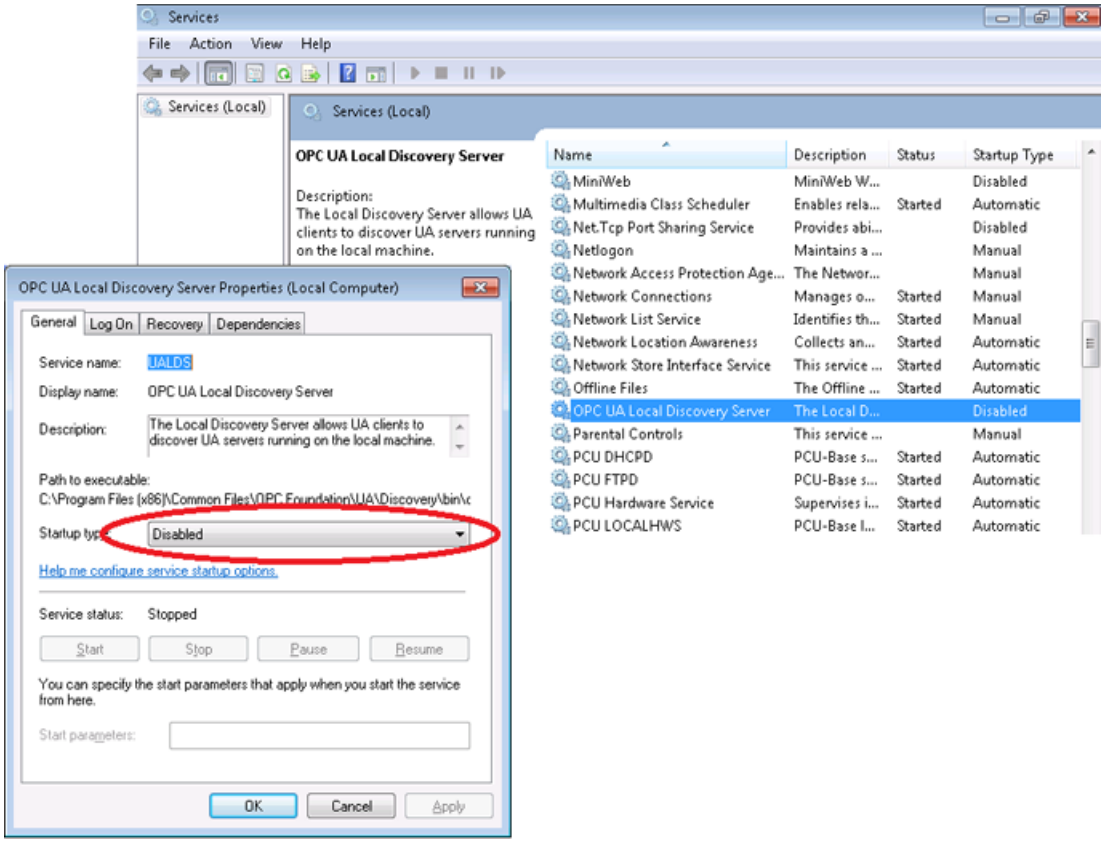


Figure 3-4 Deactivating the "OPC UA Local Discovery Server" service on PCU 50

Procedure

1. Start the OPC UA "Sample client".

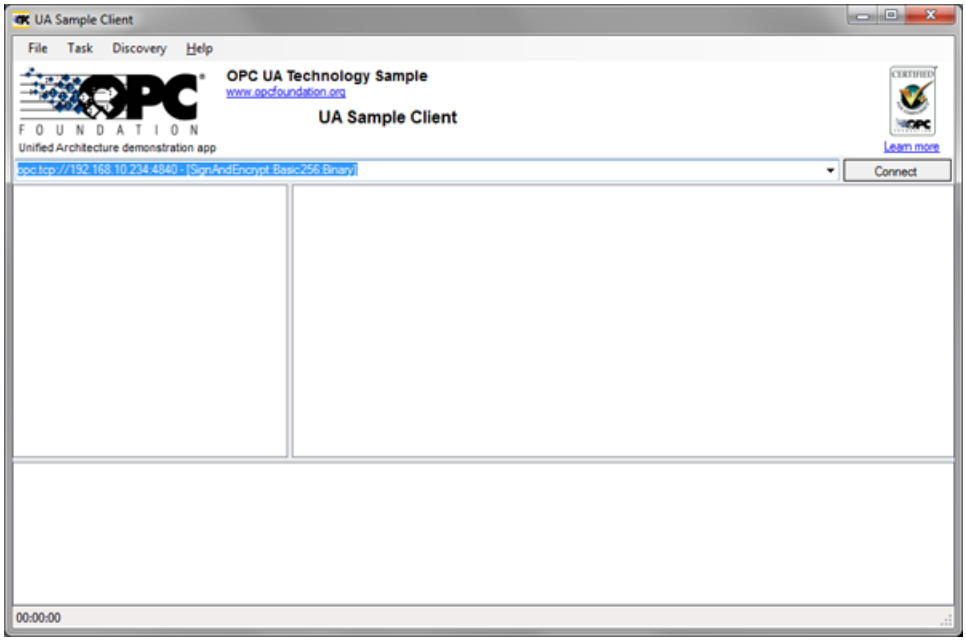


Figure 3-5 Sample Client main window

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

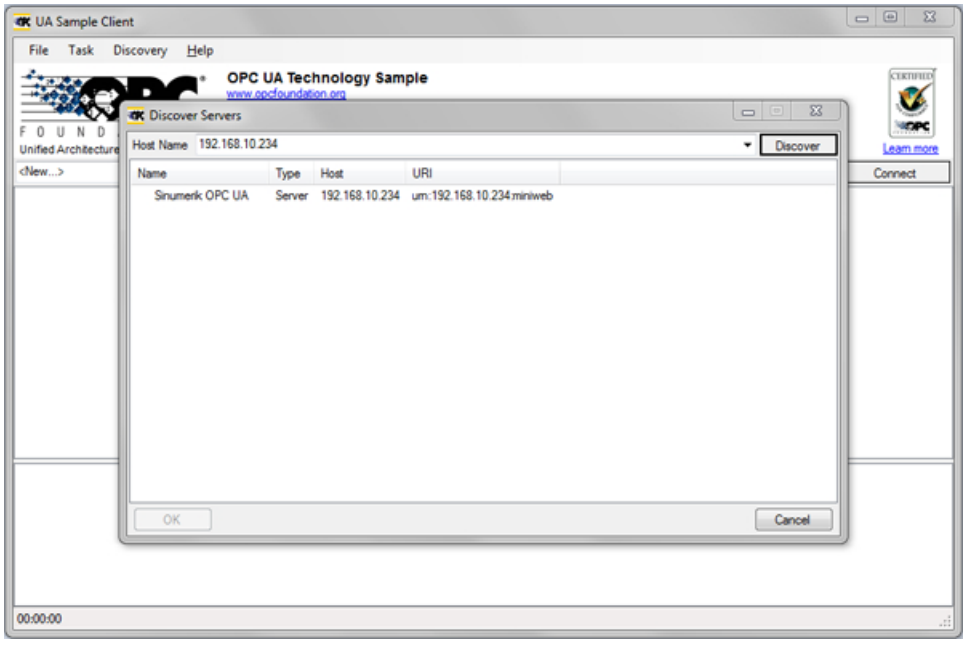


Figure 3-6 Discover servers

4. The SINUMERIK OPC UA server appears in the list. Select the server and confirm with "OK".

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

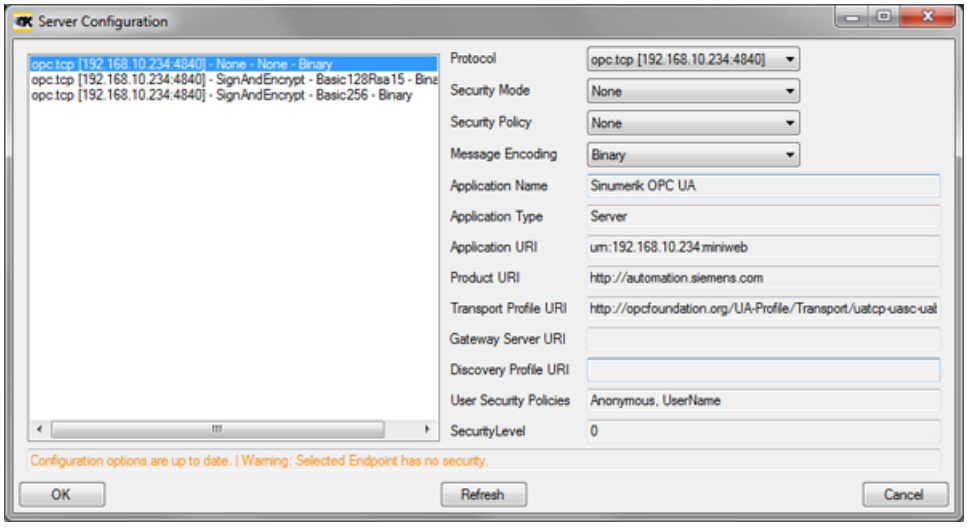


Figure 3-7 Server configuration

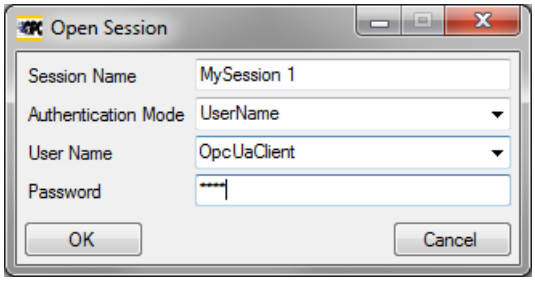


Figure 3-8 User Identity

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

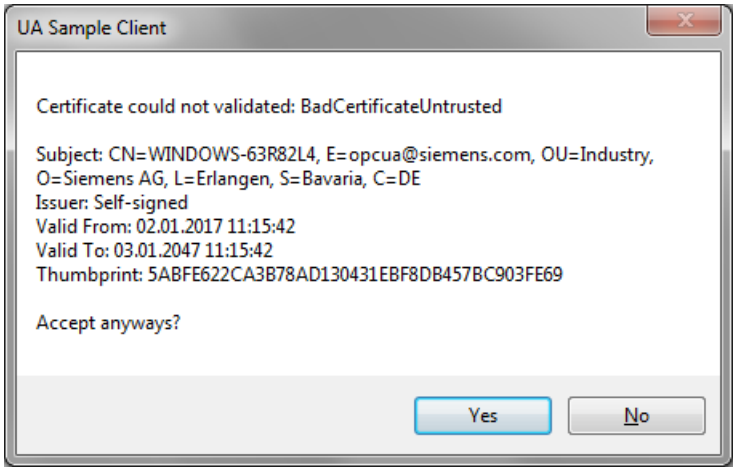


Figure 3-9 Certificate

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

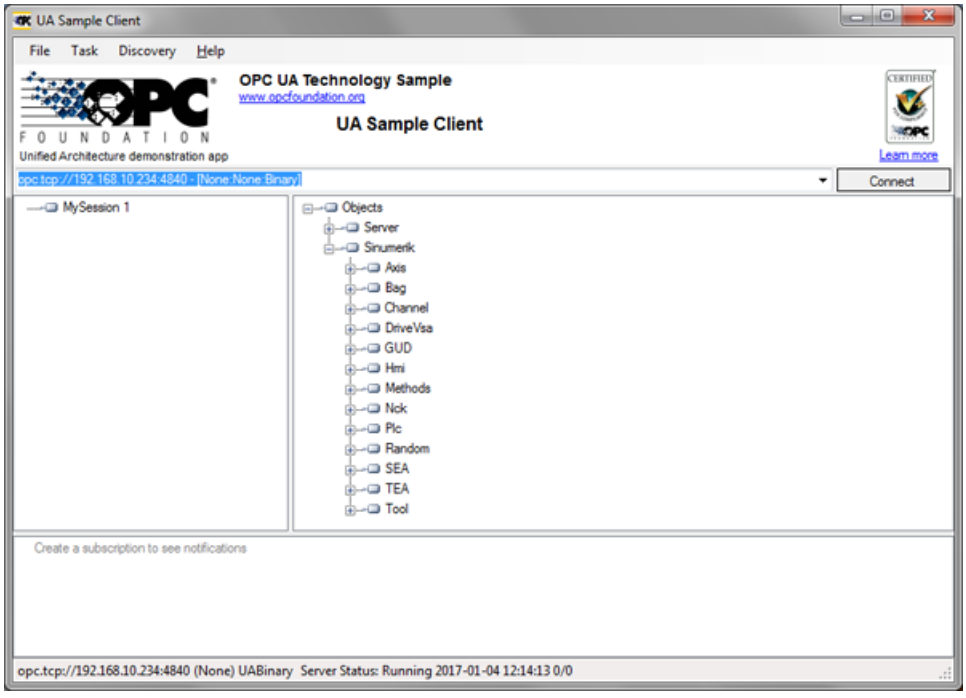


Figure 3-10 Address space of the SINUMERIK OPC UA server

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

– E.g. read, write, setup monitoring

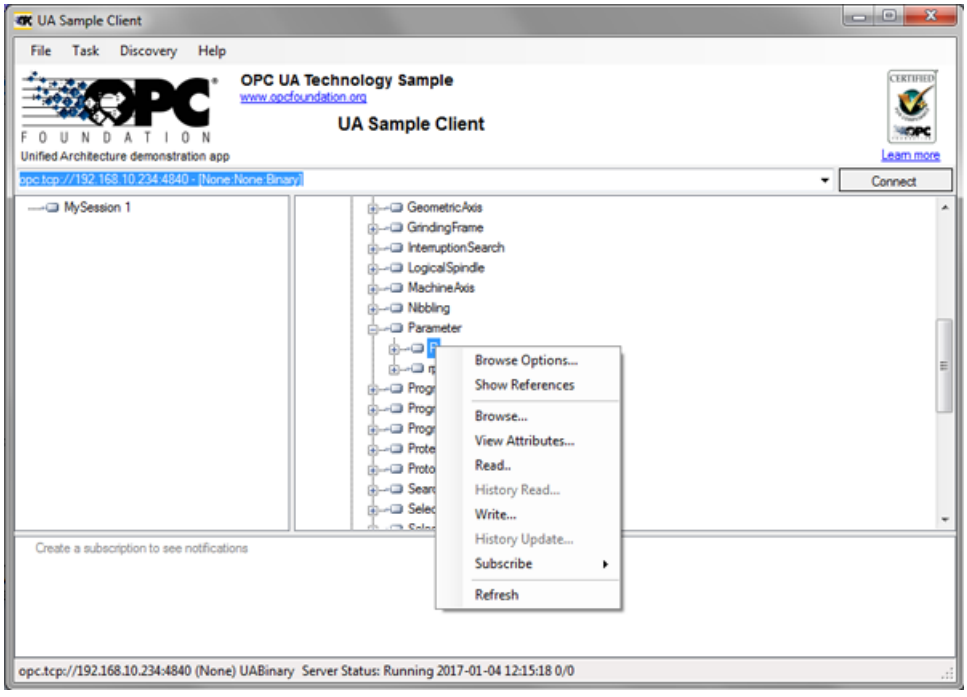


Figure 3-11 NodeID "Sinumerik > Channel > Parameter > R"

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

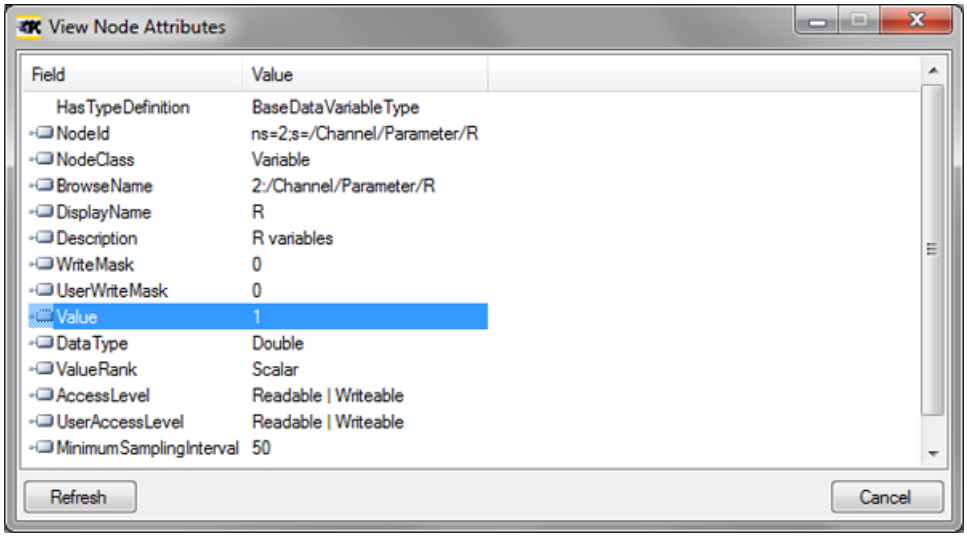


Figure 3-12 Viewing node attributes

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" 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 aguments:**	
	UserName	user, certificate is issued to
	CertficateData	Certificate(.der) as byte string
DeleteUser	Deletes a user who was added previously using the method "AddUser". **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 not write access. These rights must be explicitly set.

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
	"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
	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:**
  Transfer of part programs

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 the SINUMERIK alarm object is explained and it is shown how to get the alarms from the server.

At the end of this chapter it is explained how users can transfer files from or to the server using two comfortable methods.

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 during browsing:

- In the address space of the NC, the displayed variables always represent only the first parameter of the corresponding first OPI 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, then you must correspondingly extend the identifier; you cannot directly accept the identifiers obtained when browsing, e.g. "/Channel/Parameter/R[u2, 56]".
- In the address space of the NC, the displayed variables represent the access format that has to be extended accordingly.
  Example:
  The variable "/Plc/MB" is in the address space. This variable must be extended by the appropriate byte number, e.g. "/Plc/MB6". Only then is a value supplied.
- The address space of the NC also contains variables that are not available in a corresponding machine configuration. These variables return "BadAttributeIdInvalid" as value.

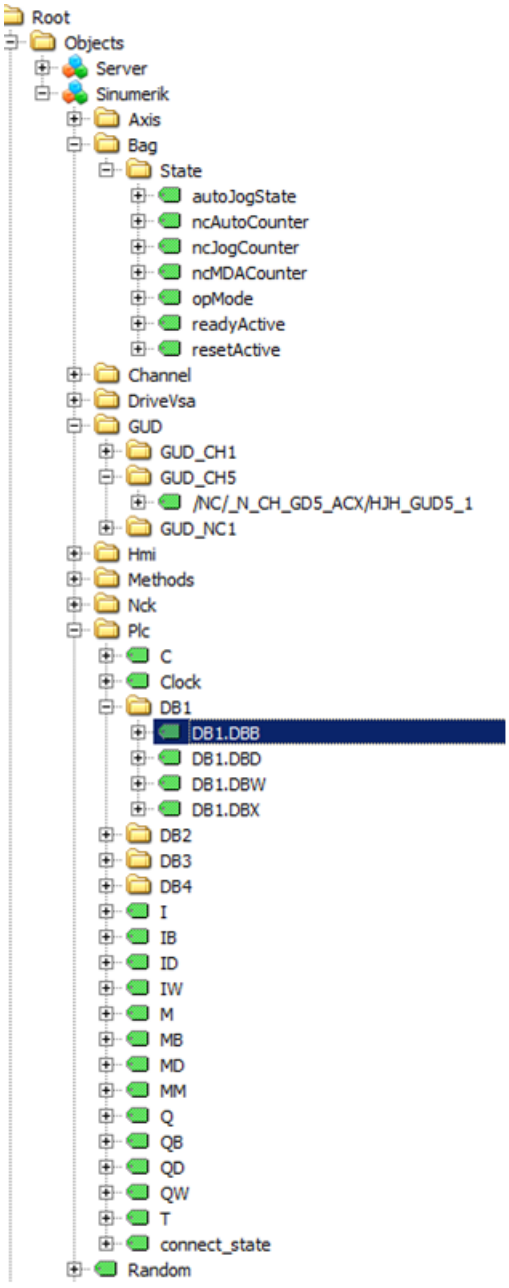


Figure 5-1 Excerpt from browsing the OPC UA data access interface

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, e.g. "/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]	R parameter array
/Channel/Parameter/R[u1,1,#5]	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

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 NC, 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". Only then a value is supplied.

Note

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

Access formats

The various access formats are shown in the following table. These must have the prefix "/Plc" added to them.

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:

- In the table, "x" stands for the byte offset in the area; "y" for the bit number in the byte; and "z" for the data block.
- The **bold data type** is the default data type in each case and does not have to be specified when addressing. In addition, the specifications DB2.DBB5.BYTE and DB2.DBB5 are equivalent, for example.
- 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
/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

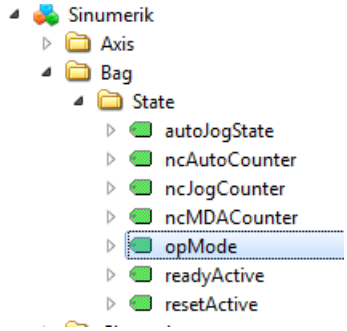
Machine data arrays are 1-indexed for access.

5.3.5 Reference of OPC UA variables

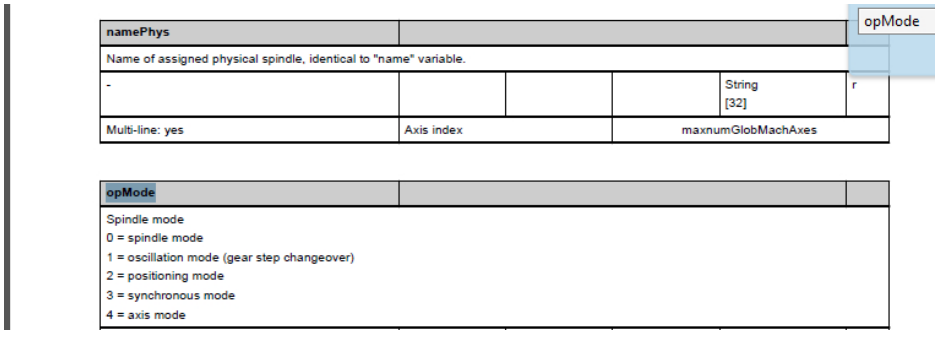
For more information on variable documentation, refer: NC variables and interface signals (https://support.industry.siemens.com/cs/de/de/view/109748365/en)

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".



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

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

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

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

   OEM-MMC: Linkitem /ToolCompensation/...

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

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

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

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

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

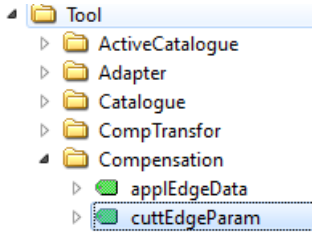
1. At the beginning of each chapter of the variable documentation you find the information "OEM-MMC: LinkItem" specifying here "/ToolCompensation/".

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

   OEM-MMC: Linkitem /ToolCompensation/...

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

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



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.

All Alarms are delivered in English language.
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".

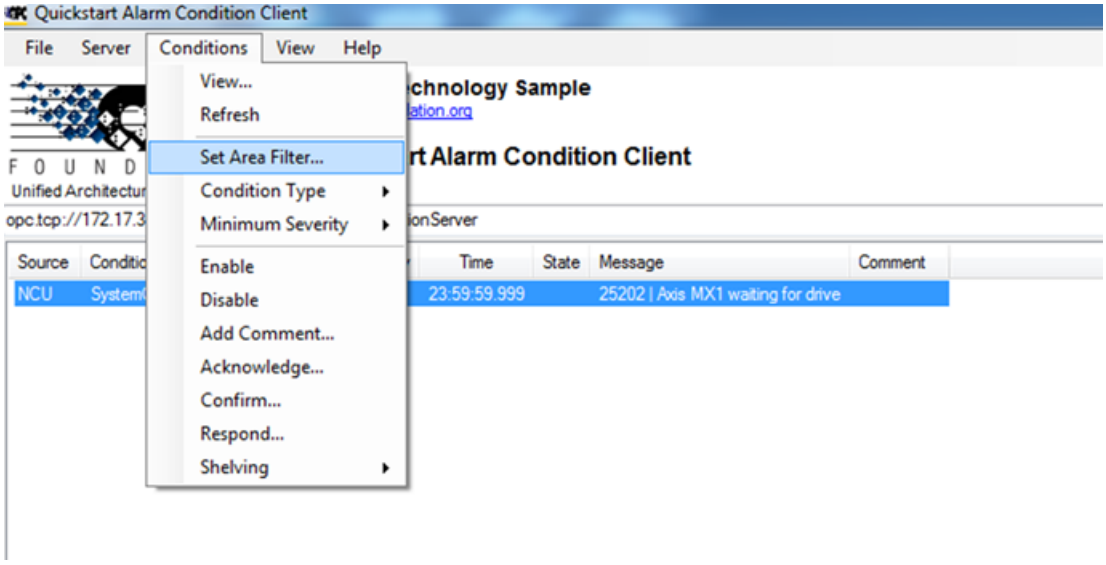


Figure 5-3 Alarm Condition Client

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

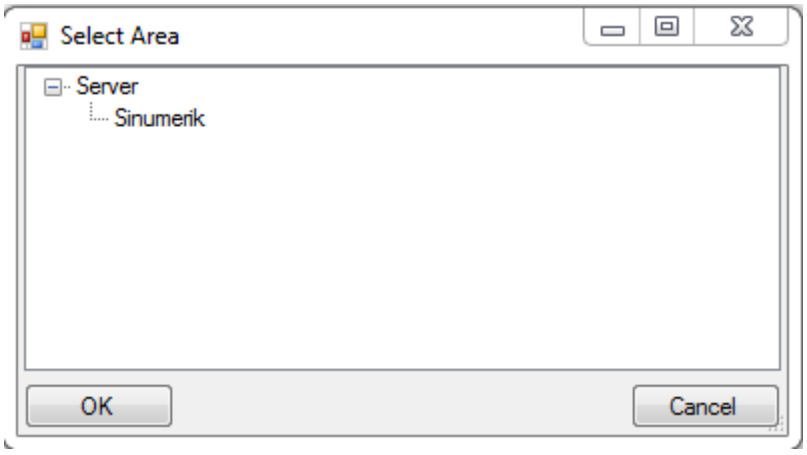


Figure 5-4 The Select Area Window

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

The alarms will be displayed on the screen.

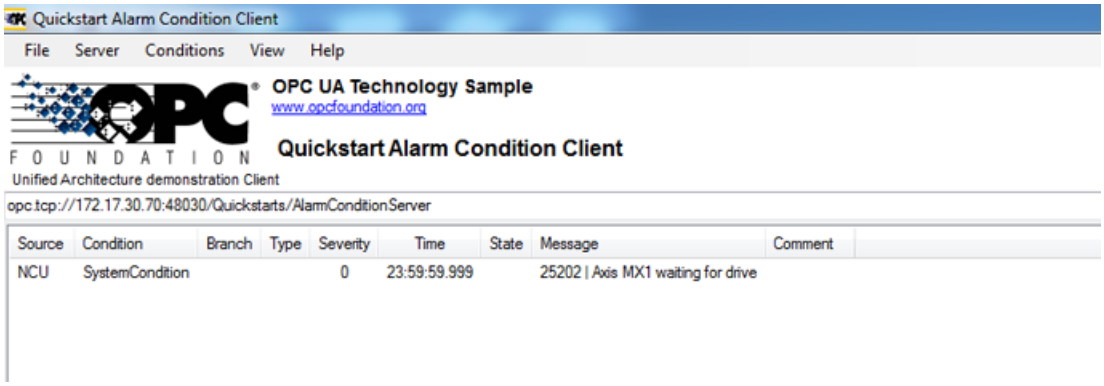


Figure 5-5 Alarm List

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 SINUMERIK Alarm object

5.4.3.1 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.

5.4.3.2 OPC UA event messages and alarms

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.

User access right is required to subscribe the Events of the Server Object. User access right with access permission has to be set to “SinuReadAll“ or “AlarmRead“.

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.

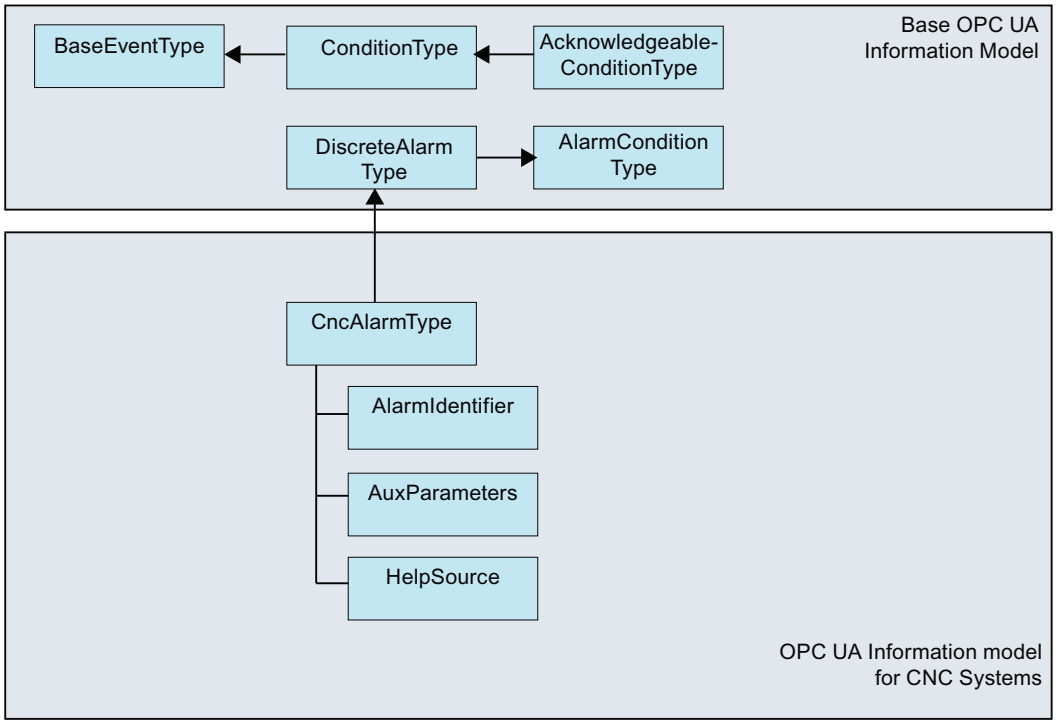


Figure 5-6 OPC UA Information Model for CNC Systems

Description of the CncAlarmType

Since the CncAlarmType is derived from a number of types as you can see in Figure 5-6, it does not only contain the three attributes AlarmIdentifier, AuxParameters and HelpSource, but also all the other attributes which are inherited from the objects, this type is derived of.

Attributes of BaseEventType

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

Severity Level	SINUMERIK System	OpcUa Server/Client
Information	0-1	1
Warning	2-999	500
Error	1000	1000

Additional attributes of the ConditionType

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

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

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

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

Additional attributes of the AcknowledgeableConditionType

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

Additional attributes of the CncAlarmType

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

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

5.4.4 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.

5.4.5 OPC UA Alarms and Conditions Constraints

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

- Acknowledgements and Confirmation of the alarms.
- Messages
- Part program messages
- Other languages except English

5.5 File transfer

5.5.1 Overview

The SINUMERIK OPC UA server offers two methods to copy NC Part programs from OPC UA Client to the SINUMERIK server and vice versa.

5.5.2 File structure

Accessing the file system

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

As a user, you will require user access rights to access these files from the server. The access rights are provided using the "GiveUserAcces" method. The following access rights can be provided for the file system (also see chapter List of rights (Page 34)):

- FSRead for the method CopyFileFromServer
- FSWrite for the method CopyFileToServer

5.5.3 Methods used to exchange the files

In addition to the standard file system, this functionality supports two additional methods to transfer the files from server to client or vice versa.

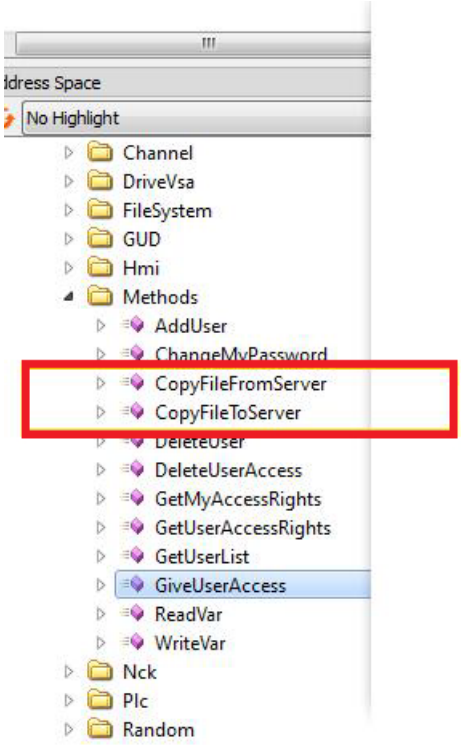


Figure 5-7 Comfort methods for the file transfer

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
in	string	SourceFile	Name of the file need to be copied with absolute path.
out	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
in	string	TargetFilename	Target file name with absolute path
in	ByteString	Data	Raw file Data
in	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
- Workpieces.

Therefore only the following main paths will be accepted by the above mentioned methods:

- Sinumerik/FileSystem/Part Program/
- Sinumerik/FileSystem/Sub Program/
- Sinumerik/FileSystem/Work Pieces/

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 Modell", Chapter 6.

This diagnostics information can be found under the Server Node:

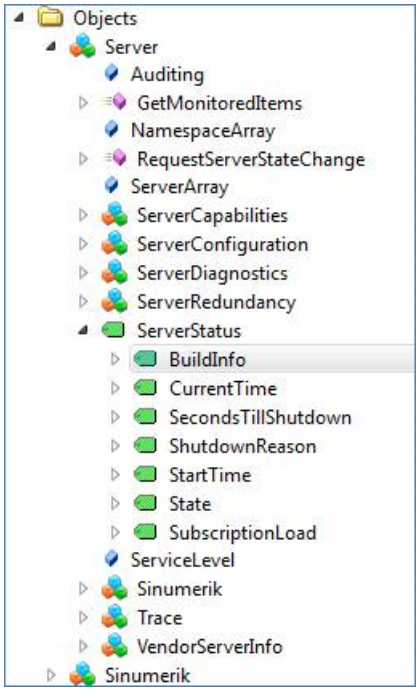


Figure 6-1 Diagnostics Information - Server Node

6.2 OPC UA server version

OPC UA server version

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

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

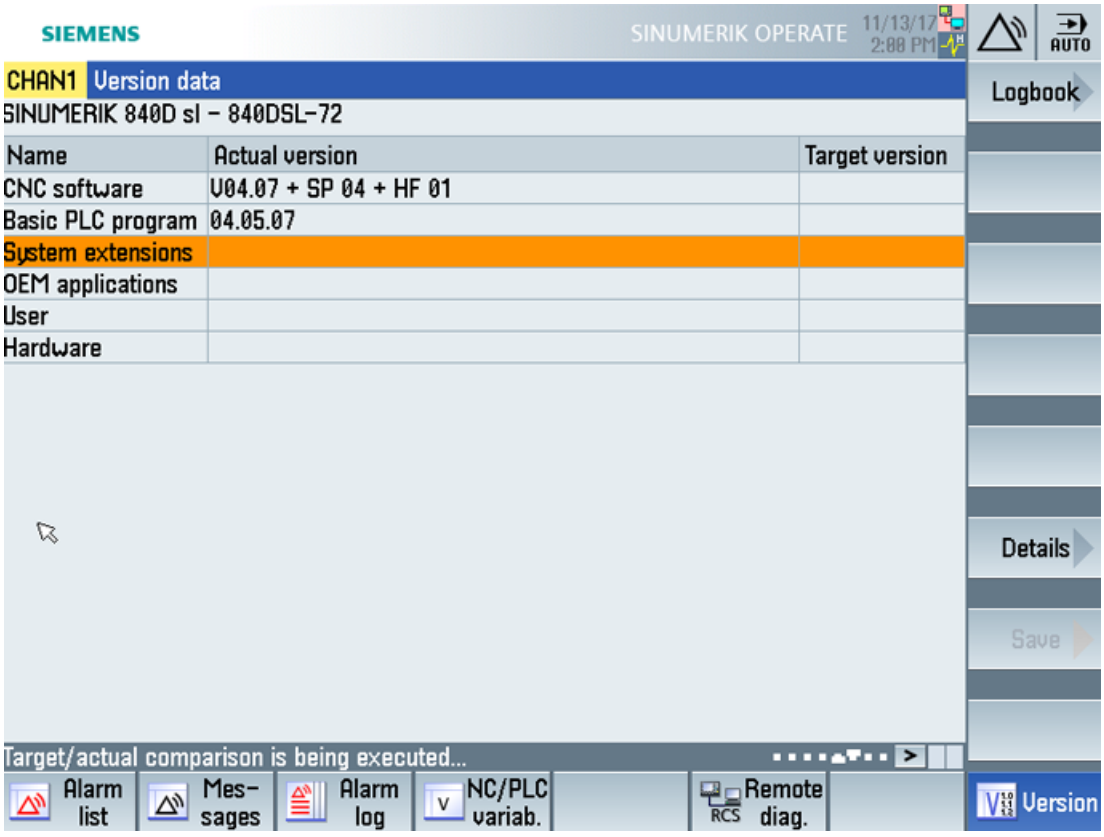


Figure 6-2 Version data

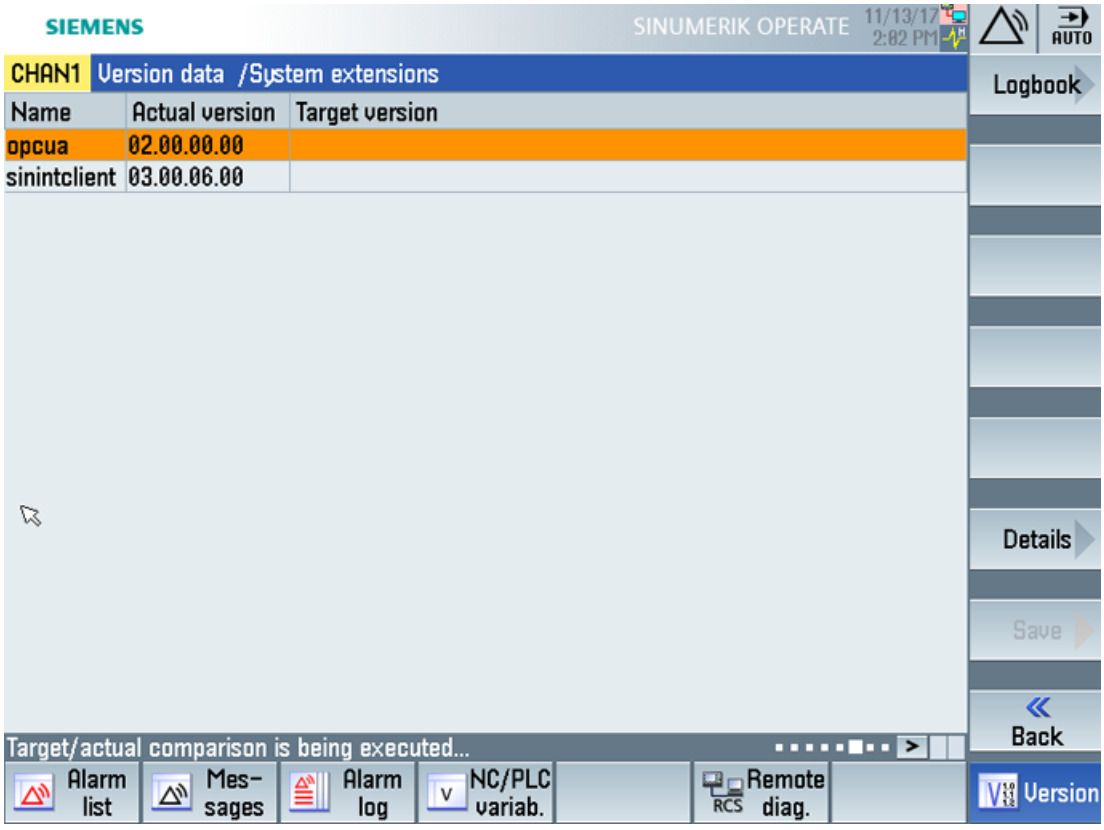


Figure 6-3 Version data / system extensions

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 Integrate Create MyConfig (CMC)

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

Release of software version

The release of new software version of OPC UA will be communicated via SINUMERIK newsletter by the SIEMENS Product Management.

7.2 Installation of OPC UA server

OPC UA - Server update

To receive the latest OPC UA server software, contact your regional SIEMENS office.

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

1. Load OPC UA software on a bootable 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	828D	5
	840 D sl	10
Number of subscriptions	828D	5
	840D sl	10
Maximum samples / second	828D	500
	840D sl	1000
Sampling rate	min. 100 ms	
Sampling interval	{100, 250, 500, 1000, 2500, 5000}	
Publishing rate	min. 100 ms	
Publishing interval	{100, 250, 500, 1000, 2500, 5000}	
Number of users	max. 20	

Calculating maximum subscription load

The maximum number of monitored items 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 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