rexroth
A Bosch Company

Application Manual

OPC UA Server App

OPC UA Server for ctrlX CORE

R911403778, Edition 06

Liability

The specified data is intended for product description purposes only and shall not be deemed to be a guaranteed characteristic unless expressly stipulated in the contract. All rights are reserved with respect to the content of this documentation and the availability of the product.

DOK-XCORE*-OPCUA*SERV*-AP06-EN-P DC-IA/EPI5 (TaDo/MePe)

f5f200cddfc773880a347e883d356b4f, 6, en_US

Table of contents

1 About this documentation

Editions of this documentation

Edition	Release date	Note
01	2020-06	First edition
02	2021-01	Revision for ctrlX CORE version UAS-V-0106
03	2021-04	Revision for ctrlX CORE version UAS-V-0108
04	2022-01	Revision for ctrlX CORE version UAS-V-0112 New: ● ➦Chapter 5.2.1 Licensing on page 21 ● ➦Chapter 5.5 Web interface on page 35 Revised: ● ➦Chapter 5.3.8 Address space of the ctrlX OPC UA Server on page 28 ● ➦Chapter 5.4 Configuration on page 29
05	2022-04	Revision for ctrlX CORE version UAS-V-0114 Revised: ● ➦Chapter 5.2 Installation on ctrlX CORE on page 19 ● ➦Chapter 5.3.5 Certificate management on page 22 ● ➦Chapter 5.3.9 Supported services for the data range Data Layer on page 29
06	2022-09	Revision for ctrlX CORE version UAS-V-0116 Revised: ● ➦Chapter 5.2 Installation on ctrlX CORE on page 19 ● ➦Chapter 5.3.5 Certificate management on page 22 ● ➦Chapter 5.3.9 Supported services for the data range Data Layer on page 29

2 Important directions on use

2.1 Intended use

2.1.1 Introduction

Rexroth products are developed and manufactured to the state-of-the-art.

The products are tested prior to delivery to ensure operational safety and reliability.

⚠ WARNING	**Personal injury and damage to property due to incorrect use of products!** The products may only be used as intended. Failure to use the products as intended may cause situations resulting in property damage and personal injury.

NOTICE	**Damages resulting from unintended use** Rexroth As the manufacturer does not assume any warranty, liability or compensatory claims for damages resulting from unintended use of the products. The user alone shall bear the risks of an unintended use of the products. Before using Rexroth products, make sure that all the prerequisites for an intended use of the products are met: – Personnel that in any way, shape or form uses Rexroth products must first read and understand the relevant safety instructions and be familiar with their intended use – Leave hardware products in their original state, i.e., do not make any structural modifications. It its not permitted to decompile software products or alter source codes – Do not install damaged or defective products or commission them – It has to be ensured that the products have been installed as described in the relevant documentation

2.1.2 Areas of use and application

Products of the ctrlX series are suitable for Motion/Logic applications.

NOTICE	Products of the ctrlX series may only be used with the accessories, mounting parts, and other components specified in this documentation. Components that are not expressly mentioned must neither be attached nor connected. The same applies to cables and lines. Only to be operated with the hardware component configurations and combinations expressly specified and with the software and firmware specified in the corresponding documentations and functional descriptions.

Products of the ctrlX series are suitable for single-axis as well as for multi-axis drive and control tasks. Device types with different equipment and interfaces are available for using the system in specific applications.

Typical areas of application:

- Building automation
- IoT and Security Gateway or Device
- Handling & Robotic

Controls of the ctrlX CORE series may only be operated under the mounting and installation conditions, in the position of normal use and under the ambient conditions (temperature, degree of protection, humidity, EMC, etc.) specified in the related documentations.

2.2 Unintended use

"Unintended use" refers to using the ctrlX products outside of the above-mentioned areas of application or under operating conditions and technical data other than described and specified in the documentation.

ctrlX products must not be used if they are exposed to following conditions:

- Operating conditions that do not meet the specified ambient conditions. Operation under water, under extreme temperature fluctuations or under extreme maximum temperatures is prohibited
- Applications that have not been expressly authorized by Rexroth

3 Safety instructions

The Safety instructions contained in the available application documentation feature specific signal words (DANGER, WARNING, CAUTION or NOTICE) and, where required, a safety alert symbol (in accordance with ANSI Z535.6-2006).

The signal word is meant to draw the reader's attention to the safety instruction and identifies the hazard severity.

The safety alert symbol (a triangle with an exclamation point), which precedes the signal words DANGER, WARNING and CAUTION, is used to alert the reader to personal injury hazards.

The Safety instructions in this documentation are designed as follows:

⚠ DANGER	In case of non-compliance with this safety instruction, death or serious injury **will** occur.
⚠ WARNING	In case of non-compliance with this safety instruction, death or serious injury **could** occur.
⚠ CAUTION	In case of non-compliance with this safety instruction, minor or moderate injury could occur.
NOTICE	In case of non-compliance with this safety instruction, property damage could occur.

4 Introduction into the OPC Unified Architecture

4.1 General information

OPC UA is the further development of the OPC industrial standard. The service-oriented architecture ensures platform independency, scalability and high-availability by omitting a DCOM basis. OPC UA ensures a complete vertical integration from the control level up to the automation component irrespective of the programming language or the operating system.OPC UA is a client/server system. Several clients can access a server simultaneously. A client can access several servers.

4.2 Overview on specifications

OPC Unified Architecture was published as multi-part specification in 14 parts by the OPC foundation ➥ http://www.opcfoundation.org. Only registered users can download the specification. Register on ➥ http://www.opcfoundation.org.

Table 1: OPC UA - Overview on specifications

Part	Specification	Download
Part 1	OPC UA Part 1 - Overview and Concepts	➥ http://www.opcfoundation.org/developer-tools/specifications-unified-architecture/part-1-overview-and-concepts/
Part 2	OPC UA Part 2 - Security Model	➥ http://www.opcfoundation.org/developer-tools/specifications-unified-architecture/part-2-security-model/
Part 3	OPC UA Part 3 - Address Space Model	➥ http://www.opcfoundation.org/developer-tools/specifications-unified-architecture/part-3-address-space-model/
Part 4	OPC UA Part 4 - Services	➥ http://www.opcfoundation.org/developer-tools/specifications-unified-architecture/part-4-services/
Part 5	OPC UA Part 5 - Information Model	➥ http://www.opcfoundation.org/developer-tools/specifications-unified-architecture/part-5-information-model/
Part 6	OPC UA Part 6 - Mappings	➥ http://www.opcfoundation.org/developer-tools/specifications-unified-architecture/part-6-mappings/
Part 7	OPC UA Part 7 - Profiles	➥ http://www.opcfoundation.org/developer-tools/specifications-unified-architecture/part-7-profiles/
Part 8	OPC UA Part 8 - Data Access	➥ http://www.opcfoundation.org/developer-tools/specifications-unified-architecture/part-8-data-access/
Part 9	OPC UA Part 9 - Alarms and Conditions	➥ http://www.opcfoundation.org/developer-tools/specifications-unified-architecture/part-9-alarms-and-conditions/
Part 10	OPC UA Part 10 - Programs	➥ http://www.opcfoundation.org/developer-tools/specifications-unified-architecture/part-10-programs/

Part	Specification	Download
Part 11	OPC UA Part 11 - Historical Access	➦ http://www.opcfoundation.org/developer-tools/specifications-unified-architecture/part-11-historical-access/
Part 12	OPC UA Part 12 - Discovery	➦ http://www.opcfoundation.org/developer-tools/specifications-unified-architecture/part-12-discovery/
Part 13	OPC UA Part 13 - Aggregates	➦ http://www.opcfoundation.org/developer-tools/specifications-unified-architecture/part-13-aggregates/
Part 14	OPC UA Part 14 - PubSub	➦ http://www.opcfoundation.org/developer-tools/specifications-unified-architecture/part-14-pubsub/

4.3 Information model

The information model of the OPC UA is based on nodes describing an object-oriented context. A node can consist of attributes, methods and events. The content depends on the "NodeClass". The type model allows to map all types of user data including meta data. Each node has a unique "NodeId". References describe the connections between nodes. ReferenceType specifies the reference semantics.

The information model of the OPC UA is used as basis and extended as individual profile by other organizations such as PLCopen. For more information on these extensions, refer to the keyword "Companion Specification" or go to the respective organizations or the OPC foundation. Each OPC UA server reports the profiles it supports upon request.

4.4 Service-oriented architecture

The OPC UA architecture is divided into logical levels.

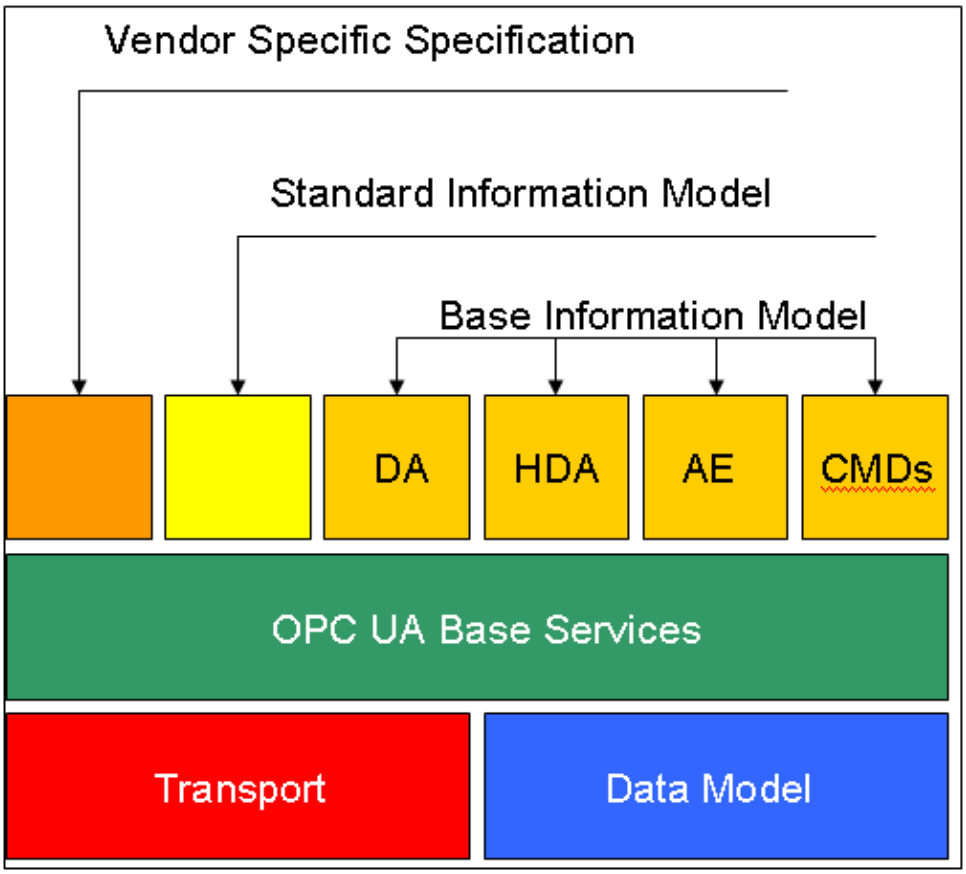

Fig. 1: OPC UA architecture

Transport level

The transport level serializes and deserializes data and sends or receives it. Data is transferred using an XML stream via the HTTP-HTTPS protocol or via a high-performance binary TCP protocol.

Basic OPC UA services

All basic OPC UA services are abstract method descriptions. They do not depend on the transport protocol and they are used as basis for all OPC UA functions. The methods are summarized in "Service Sets".

The most important "Service Sets" are mentioned in the following sections.

Discovery Service Set

The "Discovery Service Set" defines the services a client uses to determine the endpoints of a server and their security configuration. An endpoint is a variant consisting of a communication protocol, a host address, a port number and security settings.

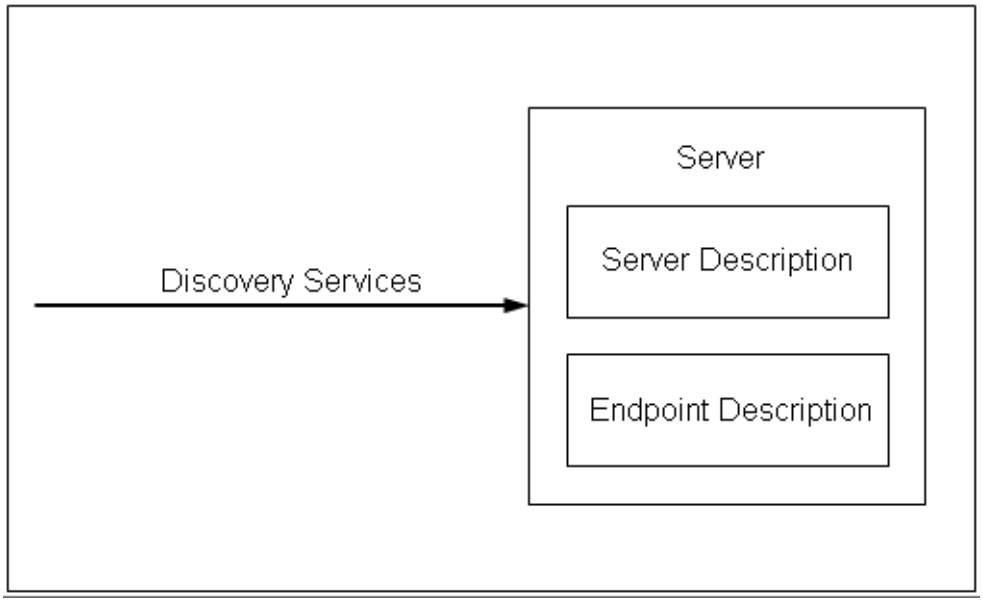

Fig. 2: Discovery Service Set

Session Service Set

A session is a logic connection between the client and the server on application level. The client can set up the connection. It can include client-specific user and language settings.

A session is set up using the "CreateSession" service. A session ID is assigned to the client. The client can use this session ID to call the following data services (Read, Write, Subscribe, etc.).

The server closes a session automatically after a client request (CloseSession) or after a timeout.

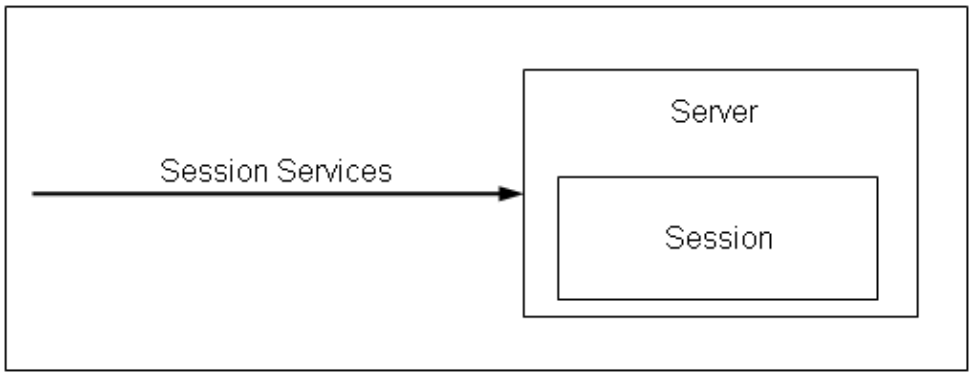

Fig. 3: Session Service Set

View Service Set

With the "View Service Set", the client allows the OPC UA server to browse through restricted address spaces (so-called views). The address space is intended to present available OPC UA server information to a client. It is generally generated from a number of nodes. The nodes are standardized objects and intended to map “Real World” objects.

Most important node classes:

- Variable
- Object
- Method

The connections between the nodes are set up using references. It is differentiated between hierarchical and non-hierarchical references. Hierarchical references are used to map a structural node order for example. Non-hierarchical references are used to refer to a node type definition for example.

The type system of nodes and references include types for objects, references, variables, events and data. This type system can be extended by the derivation of existing types and thus be provided with deeper semantics.

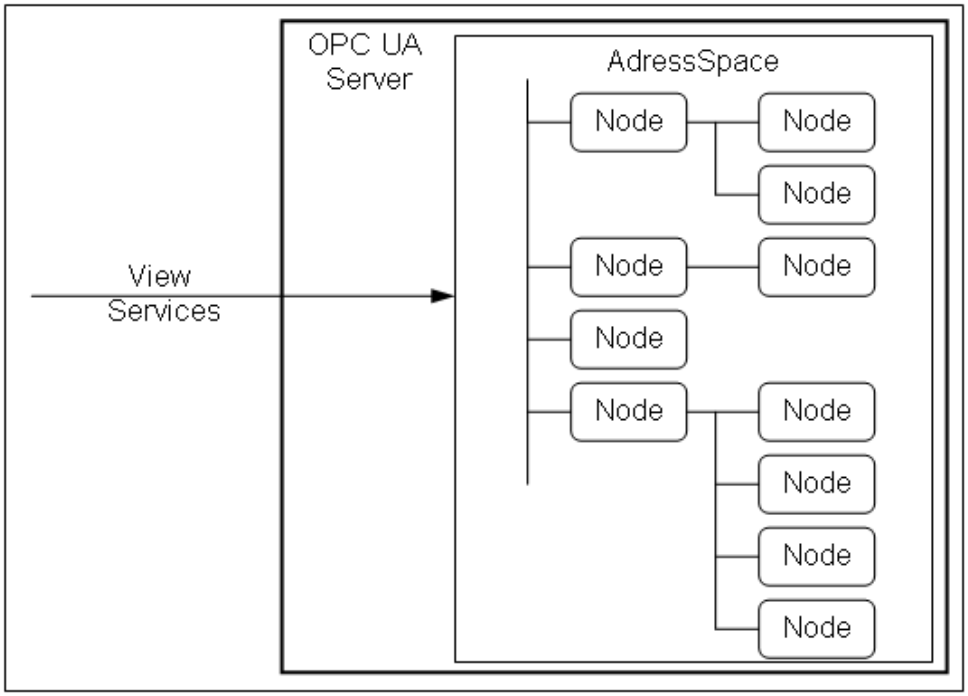

Fig. 4: View Service Set

Attribute Service Set

A node consists of multiple attributes. These attributes describe a node in detail. The node class specifies the attributes of a node. Only nodes of the "Variable" node class contain the attribute "Value".

All node classes have a common set of basic attributes. The basic attributes are for example “NodeId” to uniquely address a node, "NodeClass" and "BrowseName".

Read-only and write access is provided for these attributes using the "Service Set" attribute.

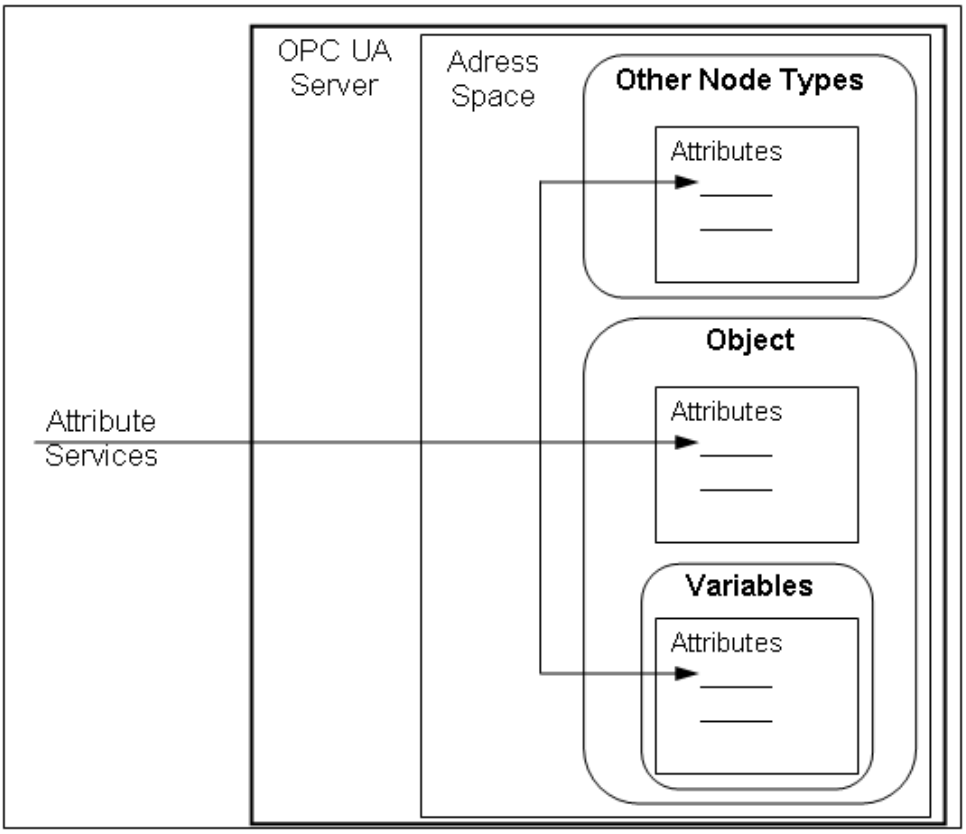

Fig. 5: Attribute Service Set

Subscription Service Set

Subscriptions are an efficient method in the OPC UA to receive information on value changes in the OPC UA server from the server. Clients can create, modify and delete subscriptions using the "Subscription Service Set"

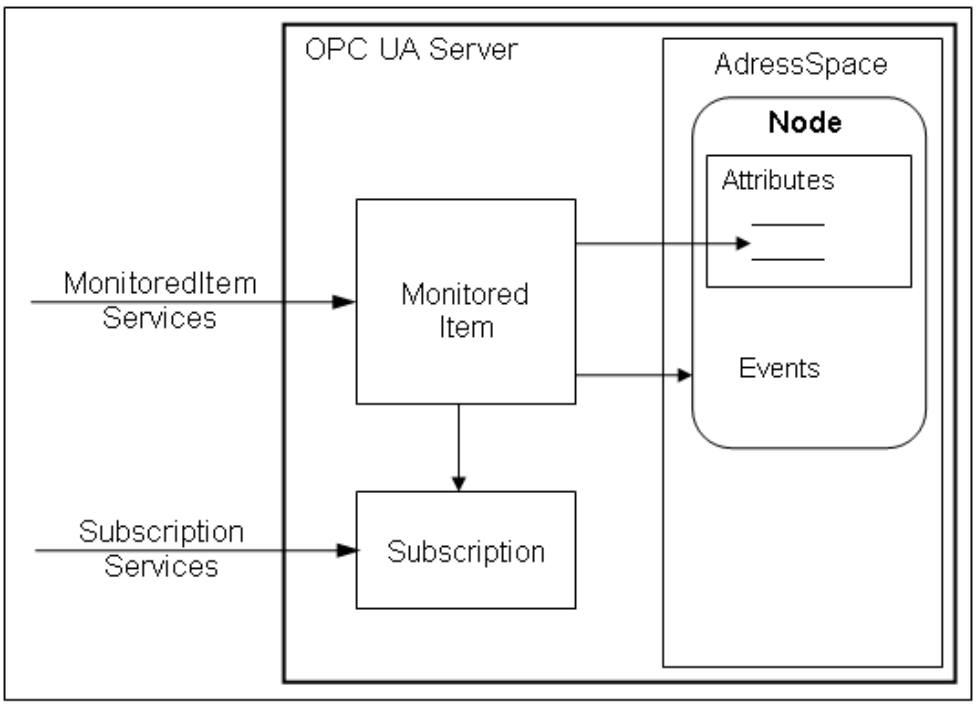

Fig. 6: Subscription Service Set

MonitoredItem Service Set

A "MonitoredItem" is a "Value" attribute, an aggregation of one or several "Value" attributes or an event included in a subscription. If the value of these "Value" attributes changes or if a corresponding event is reported, this value is transferred automatically to the client.

Clients can create, modify or delete "MonitoredItems" in the OPC UA server using the "MonitoredItem Service Set".

5 Rexroth ctrlX OPC UA Server

5.1 The ctrlX OPC UA Server in the ctrlX AUTOMATION

The ctrlX OPC UA Server runs as individual app in the ctrlX CORE.

Install the app on the ctrlX CORE to add the standard communication protocol OPC UA to the ctrlX. Thus, the access to the control is standardized. The ctrlX backend Data Layer is used to access ctrlX CORE data. This ensures that all data of the apps installed on the ctrlX CORE is also available via the ctrlX OPC UA Server.

The app “OPC UA Server“ is not installed on the ctrlX CORE by default. Thus, install it first on the ctrlX CORE.

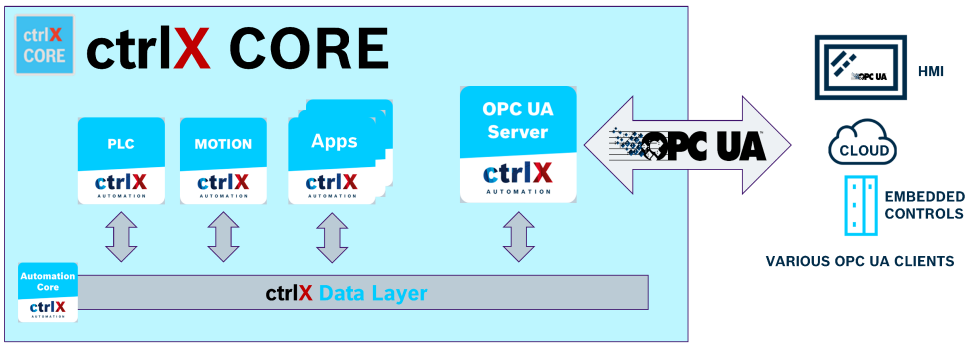

Fig. 7: ctrlX OPC UA Server in the ctrlX CORE

5.2 Installation on ctrlX CORE

Install the app “OPC UA Server“ on the ctrlX CORE before using the ctrlX OPC UA Server. Use the package manager of the ctrlX CORE. The installation does not depend on other apps. All data ranges of the apps installed on the ctrlX CORE are shown. The installation takes a few minutes. For a successful installation, the apps Device Admin and Automation Core have to be already installed on the ctrlX CORE. It can only be installed in the “Service Mode". After the installation, return to the “Operation Mode” to provide control data in the ctrlX OPC UA Server.

To install on the ctrlX CORE, the user needs the user permission “Apps: Manage apps" or "Administration: Full Access".

For the Package Manager, go to the web interface under *“Settings → Apps”*.

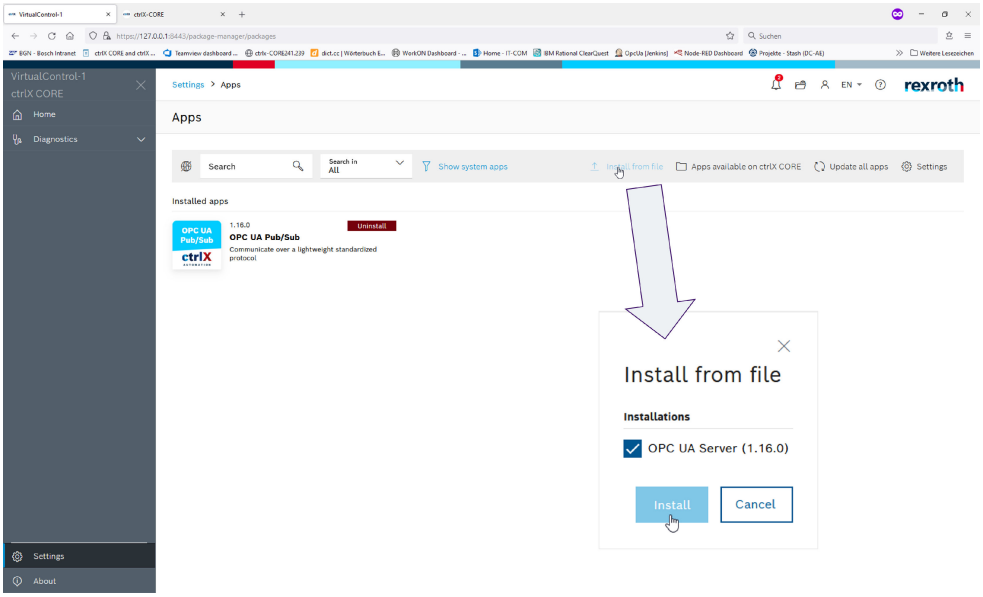

Fig. 8: For the installation of the app "OPC UA Server", go to *“Settings → Apps”*

To install the app "OPC UA Server", use the web engineering interface.

To install, proceed with the following steps as shown in Fig. 8:

1. Select “Apps” from the “Settings” menu
2. Select Install from file to install the app from the file system
3. Select the installation file.
4. Install via the button “Install”.

After installing the app “OPC UA Server“ and before using the app for the first time, set the respective permission in the Identity Manager under *“Settings → Users & Permissions → Permissions”*.

Fig. 9: Identity manager under *“Settings → Users & Permissions → Permissions”*

The user "boschrexroth" is already selected for permission.

All users with one of the following permissions can access the ctrlX OPC UA Server:

- " OPC UA Scopes: OPC UA Server access"
- "Administration: Full Access"

The permission can also be set when configuring a user.

5.2.1 Licensing

A valid license is required to use the OPC UA Server. This license can be loaded before or after the license.

To operate the ctrlX OPC UA Server, one of the following licenses is required:

- SWL_XCR_ENGINEERING_4H
- SWL-XCx-UAS-OPCUASERVERxx-NNNN

The ctrlX OPC UA Server can be configured without license via the web interface of the control. However, it cannot be connected to the control in this state via the OPC UA.

Further information

- ctrlX CORE Runtime, Application Manual, chapter "ctrlX licenses" (R911403768, DOK-XCORE*-BASE*******-APRS-EN-P)
- ctrlX Automation website

5.3 Properties

5.3.1 Connection settings

To go to the ctrlX OPC UA Server, use the engineering interface of the ctrlX CORE.

The OPC UA server uses the port 4840 by default.

EndpointURL structure:**opc.tcp://<HostNameOfThe Control>:4840** or **opc.tcp://<HostAddress>:4840**.

The default IP address of the ctrlX CORE (192.168.1.1) corresponds to die EndpointURL **opc.tcp://192.168.1.1:4840**.

5.3.2 Security

The following methods to encrypt and sign (SecurityPolicies) are enabled by default:

- **SecurityPolicy [B] – Basic256Sha256**
- **SecurityPolicy [A] - Aes128-Sha256-RsaOaep**
- **SecurityPolicy - Aes256-Sha256-RsaPss**

Use the Aes256-Sha256-RsaPss method if possible, as it is the most secure method.

An unencrypted connection (SecurityPolicy None) can be enabled via the configuration.

An unencrypted connection is only recommended for diagnostic purposes.

The unencrypted connection should not be used for the general operation.

5.3.3 Endpoints

The following endpoints with different methods to encrypt and sign are available by default:

- **Sign –Basic256Sha256**
- **Sign – Aes128-Sha256-RsaOaep**

- **Sign – Aes256-Sha256-RsaPss**
- **SignAndEncrypt –Basic256Sha256**
- **SignAndEncrypt – Aes128-Sha256-RsaOaep**
- **SignAndEncrypt – Aes256-Sha256-RsaPss**

5.3.4 User und password

To connect to the ctrlX OPC UA Server, a valid combination consisting of username and password is required. Use the ctrlX CORE Identity Manager to configure username and password (under *“Settings → User & Permissions”* in the web interface)

The user has to have one of the following permissions:

- OPC UA Scopes: OPC UA Server access
- Administration : Full access

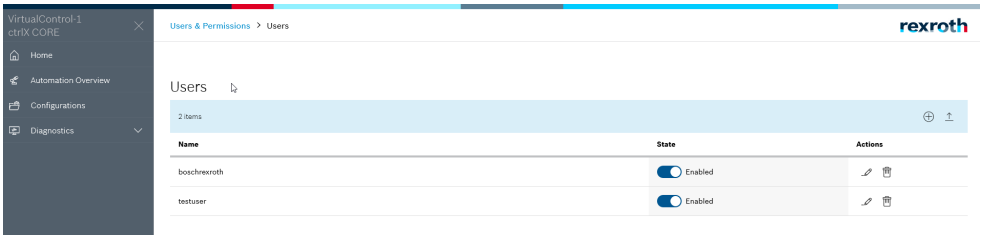

Fig. 10: Example configuration of a user in the ctrlX CORE Identity Manager

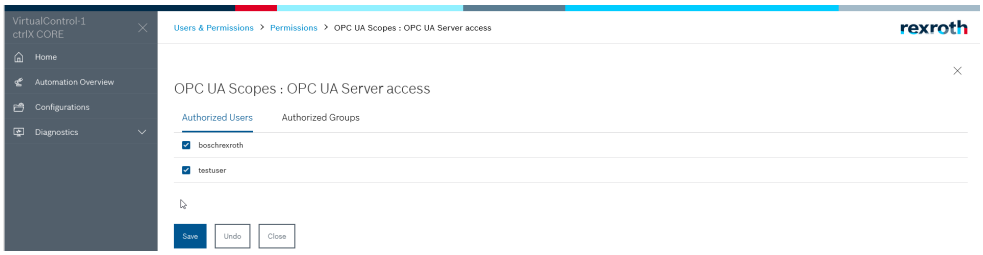

Fig. 11: Example configuration of the permissions in "OPC UA Scopes: OPC UA Server access"

To send the password to the control, the following two UserNameIdentityTokens are provided by default:

- **"Username_256_Token” with SecurityPolicy BASIC256SHA256}**
- **"Username_256_RSAPSS_Token” with SecurityPolicy Aes256-Sha256-RsaPss**

Username_256_Token with SecurityPolicy BASIC256SHA256 is also the standard method of SecurityPolicy Aes128-Sha256-RsaOaep.

The AnonymousIdentityToken "Anonymous_Token" is provided for the FindServer & Get Endpoint services. Username and password are required to set up an OPC UA session. An anonymous access is not possible.

5.3.5 Certificate management

A secure connection between the OPC UA server and the client is based on trustworthy certificates. Currently, only the self-signed certificate management is supported. There is based on a manual exchange of certificates between the OPC UA server and the client. Certificates are exchanged when establishing a connection between the client and the server. Server and client have to trust the certificates manually.

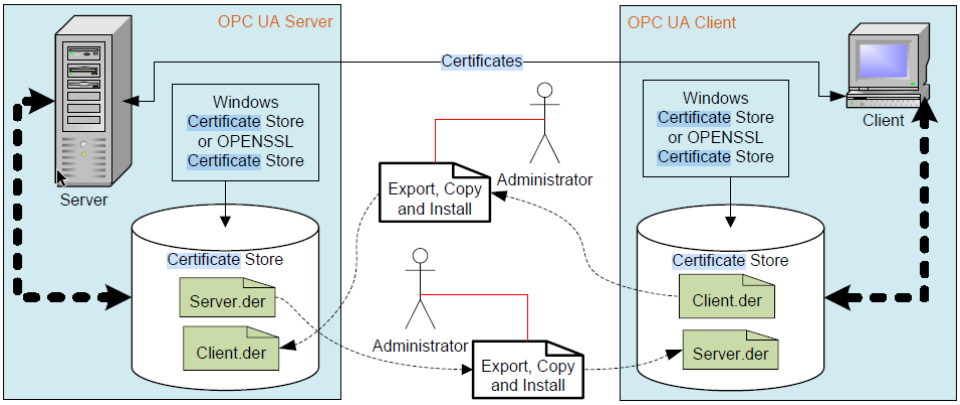

Fig. 12: Manual certificate management from “OPC UA Specification Part 2: Security“

For the ctrlX OPC UA Server, the certificates are trusted via the ctrlX CORE Certificate Manager (under *“Settings → Certificates & Keys”* in the web interface).

The following steps are required:

1. First, set up a secure connection (SecureChannel) using the OpenSecureChannel. The certificate is transferred from the client to the server.
   ➡ The server reports the error "BadSecurityChecksFailed" and enters the client certificate into its “Reject" list for certificates.
2. The certificate of the client is shown as “rejected" in the Certificate Manager under *“Certificates & Keys → OPC UA Server”*. This certificate can be trusted manually. The client has to trust the server certificate as well.
3. The client can now set up a secure OPC UA connection to the server.

The certificate of the client can also be uploaded directly in the Certificate Manager. Thus, step 1 is omitted. However, the certificate has to be renamed before. The file name has to correspond to the SHA1 value of the file. This can for example be determined using the fingerprint of the certificate. When renaming, all characters of the SHA1 have to be shown in capitals. The file schema is "*[SHA1 value capitalized]*.der".

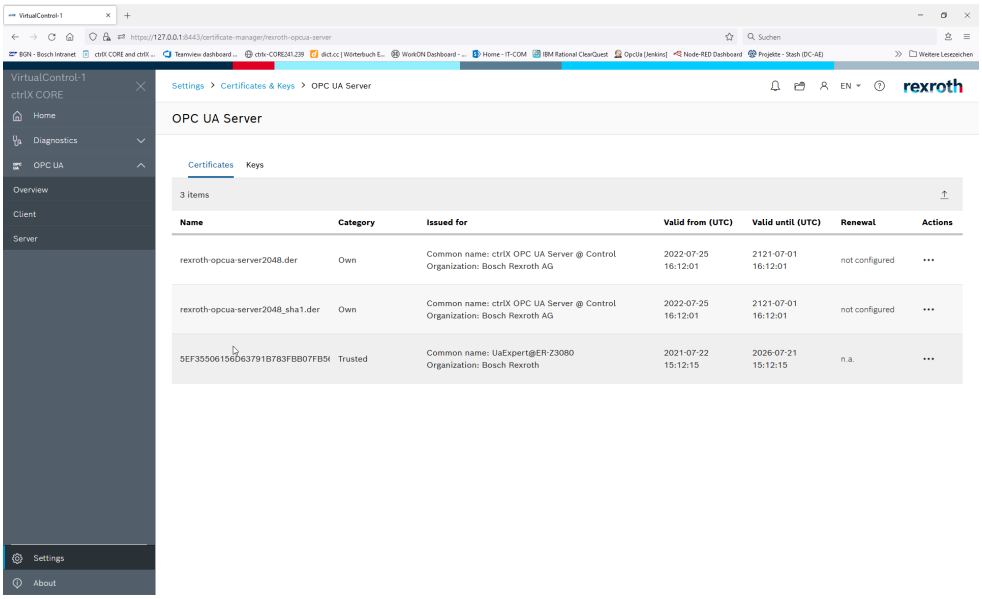

Fig. 13: Certificate Manager for the ctrlX OPC UA Server

Technical information on certificates

The certificates of the ctrlX OPC UA Server are currently self-generated and signed and valid for 36135 (ca. 99 year) by default.

The encryption method used is "sha256" and "sha1".

Technical information on the storage of certificates

Certificates are stored in the Certificate Store.

For the Certificate Store, go to *$SNAP_COMMON/package-certificates/rexroth-opcua-server/rexroth-opcua-server/*.

The path for VirtualControl is for example:

/var/snap/rexroth-opcua-server/common/package-certificates/rexroth-opcua-server/rexroth-opcua-server/

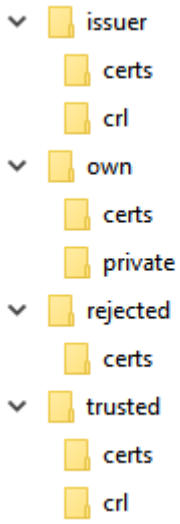

Fig. 14: Certificate Store - Folders and subfolders

The Certificate Store consists of the following folders:

- issuer:
  Currently not supported
- own:
  Includes the Application Instance Certificate from the OPC UA server or client and the respective private keys
- rejected:
  Includes certificates from the UA client or server that intend to set up a connection to the OPC UA server or client, but they have not yet been trusted
- trusted:
  Includes certificates of the UA client or servers. The OPC UA server or client trusts these certificates
  The respective subfolder “certs“ includes the certificates belonging to the individual categories, e.g. which certificates can be trusted (below the folder “trusted“) and which cannot be trusted (below the folder “rejected“). There is a Certificate Revocation List (CRL) in the subfolder “crl“.

5.3.6 Protocol and encoding

The following is supported as per the profile of the OPC UA standard release 1.04 (Part 7 - Profiles):

Table 2: ctrlX OPC UA Server - Supported profiles

Protocol and Encoding		
Name	**Description**	**From Profile**
Protocol UA TCP	Support the UA TCP transport protocol defined in UA Part 6.	UA-TCP UA-SC UA-Binary
UA Secure Conversation	Support UA Secure Conversation specified in UA Part 6.	UA-TCP UA-SC UA-Binary
UA Binary Encoding	Support UA Binary Encoding. Values of these data types are encoded in compact binary formats, contiguously and without tagging. I.e. the receiver is assumed to understand the structure it is decoding.	UA-TCP UA-SC UA-Binary

5.3.7 Supported services

The following services are supported as per the profile of the OPC UA standard release 1.04 (Part 7 - Profiles):

Table 3: ctrlX OPC UA Server - "Discovery Services"

Discovery Services		
Name	**Description**	**From Profile**
Discovery Get Endpoints	Support the GetEndpoints Service to obtain all Endpoints of the Server. This includes filtering based on Profiles.	Core 2017 Server Facet
Discovery Find Servers Self	Support the FindServers Service only for itself	Core 2017 Server Facet

Table 4: ctrlX OPC UA Server - "Session Services"

Session Services			
Name	**Description**	**From Profile**	**Comments**
Session General Service Behaviour	Implement basic Service behaviour. This includes in particular: • checking the authentication token • returning the requestHandle in responses • returning available diagnostic information as requested with the 'returnDiagnostics' parameter • respecting a timeoutHint	Core 2017 Server Facet	

Session Services			
Name	**Description**	**From Profile**	**Comments**
Session Base	Support the Session Service Set (CreateSession, ActivateSession, CloseSession) except the use of ActivateSession to change the Session user. This includes correct handling of all parameters that are provided. Note that for the CreateSession and ActivateSession services, if the SecurityMode = None then: 1) The Application Certificate and Nonce are optional. 2) The signatures are null/empty. The details of this are described in Part 4.	Core 2017 Server Facet	
Session Minimum 1	Support minimum 1 Session (total)	Core 2017 Server Facet	Max. 12 Sessions Max. 10 Sessions for Subscriptions
Session Minimum 2 Parallel	Support minimum 2 parallel Sessions (total for all Clients)	Micro Embedded Device 2017 Server Profile	Max. 12 Sessions Max. 10 Sessions for Subscriptions

Table 5: ctrlX OPC UA Server - "View Services"

View Services			
Name	**Description**	**From Profile**	**Comments**
View Basic	Support the View Service Set (Browse, BrowseNext)	Core 2017 Server Facet	
View TranslateBrowsePath	Support TranslateBrowsePathsToNodeIds Service	Core 2017 Server Facet	

Table 6: ctrlX OPC UA Server - "Attribute Services"

Attribute Services		
Name	**Description**	**From Profile**
Attribute Read	Supports the Read Service to read one or more Attributes of one or more Nodes. This includes support of the IndexRange parameter to read a single element or a range of elements when the Attribute value is an array	Core 2017 Server Facet
Attribute Write Values	Supports writing to values to one or more Attributes of one or more Nodes	Core 2017 Server Facet

Table 7: ctrlX OPC UA Server- "Supscription Services"

Subscription Services			
Name	**Description**	**From Profile**	**Comments**
Subscription Basic	Support the following Subscription Services: CreateSubscription, ModifySubscription, DeleteSubscriptions, Publish, Republish and SetPublishingMode	Embedded DataChange Subscription Server Facet	

Subscription Services			
Name	**Description**	**From Profile**	**Comments**
Subscription Minimum 05	Support at least 5 Subscriptions per Session. This number has to be supported for at least half of the minimum required sessions.	Enhanced DataChange Subscription 2017 Server Facet	Max 10. Subscriptions per Session
Subscription Publish Min 10	Support at least 10 Publish Service requests per Session. This number has to be supported for at least half of the minimum required sessions. Support, as a minimum, the number of Publish requests per session as the size of the NotificationMessage retransmission queue for Republish.	Enhanced DataChange Subscription 2017 Server Facet	Max 10. Publish Service requests per Session
Subscription Publish Discard Policy	Respect the specified policy for discarding Publish Service requests. If the maximum number of Publish Service requests has been queued and a new Publish Service request arrives, the "oldest" Publish request has to be discarded by returning the proper error.	Embedded DataChange Subscription Server Facet	

Table 8: ctrlX OPC UA Server- "Monitored Item Services"

Monitored Item Services			
Name	**Description**	**From Profile**	**Comments**
Monitor Basic	Support the following MonitoredItem Services: CreateMonitoredItems, ModifyMonitoredItems, DeleteMonitoredItems and SetMonitoringMode	Embedded DataChange Subscription Server Facet	
Monitor Value Change	Support creation of MonitoredItems for Attribute value changes. This includes support of the IndexRange to select a single element or a range of elements when the Attribute value is an array	Embedded DataChange Subscription Server Facet	

Monitored Item Services			
Name	**Description**	**From Profile**	**Comments**
Monitor Items 500	Support at least 500 MonitoredItems per Subscription. This number has to be supported for at least half of the required subscriptions for half of the required sessions.	Enhanced DataChange Subscription 2017 Server Facet	Max 500 pro Session. 5000 across all 10 Sessions
Monitor MinQueue-Size_05	Support at least 5 queue entries for MonitoredItems. Servers often will adapt the queue size to the number of currently MonitoredItems. However, it is expected that Servers support this minimum queue size for at least one third of the supported MonitoredItems.	Enhanced DataChange Subscription 2017 Server Facet	Max Queue size: 100

Table 9: ctrlX OPC UA Server- "Method Services"

Method Services				
Name	**Description**	**From Profile**	**Test Cases**	**Comments**
Method Call	Support the Call Service to call (invoke) a Method which includes support for Method Parameters.	Standard DataChange Subscription 2017 Server Facet	Open	Only partially supported in the data range of the Data Layer

5.3.8 Address space of the ctrlX OPC UA Server

Currently, there are seven namespaces in the ctrlX OPC UA Server:

Table 10: ctrlX OPC UA Server - Namespaces

Namespace Index	Namespace Url
0	http://opcfoundation.org/UA/
1	urn:Control@Rexroth:ctrlX:AUTOMATION:Server
2	http://www.boschrexroth.com/OpcUa/Datalayer
3	http://www.boschrexroth.com/OpcUa/DatalayerTypes
4	http://www.boschrexroth.com/OpcUa/DatalayerEncoding
5	Reserved for reloadable information models
6	http://www.boschrexroth.com/OpcUa/DatalayerMethod
7	http://www.boschrexroth.com/OpcUa/DatalayerEnumeration
8	http://www.boschrexroth.com/OpcUa/DatalayerObjects
9	http://www.boschrexroth.com/OpcUa/DatalayerInputArguments
10	http://www.boschrexroth.com/OpcUa/DatalayerOutputArguments

Namespaces 2 to 4 provide data for the Data Layer, its types and encoding of structures in the Data Layer.

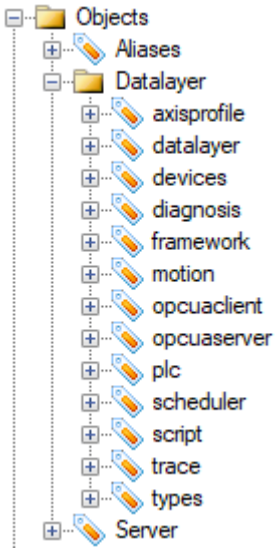

Fig. 15: ctrlX OPC UA Server - Address space under "Objects"

All user data of the control is below the node *Objects/DataLayer/*. Child data is directly mapped to the Data Layer. This area is adjusted dynamically depending on the installed snaps.

In the Fig. 15 for example, all data of the apps Automation Core, Motion, OPC UA Server and OPC UA Client is available.

5.3.9 Supported services for the data range Data Layer

Supported services for the Data Layer data range:

- **Browse und TranslateBrowsePathsToNodeIds**
- **Read**
- **Write**
- **Subscription**
  The following restrictions apply:
  - First change in data after the sampling interval
- **Call**
  The following restrictions apply:
  - Structures are not supported as parameters (InputArguments and OutputArguments)

5.4 Configuration

The ctrlX OPC UA Server can be configured with the version 1.6.0 using the Data Layer. As shown in Fig. 16, all configuration parameters and configuration functions are below the Data Layer item "*opcuaserver*". A changed configuration is applied upon the next restart of the ctrlX Core OPC UA Server

The configuration also includes parameters for sessions, subscriptions, SecurityPolicies and endpoints.

In 1.12.0, basic parameters can also be configured via the web interface, see section ➥ Chapter 5.5 Web interface on page 35.

An initial configuration is not required. The OPC UA Server app has a default configuration that allows an immediate server operation.

The OPC UA server might not be reachable anymore due to an incorrect configuration. In this case, either undo the change via the Data Layer or uninstall the ctrlX app OPC UA Server and install it again.

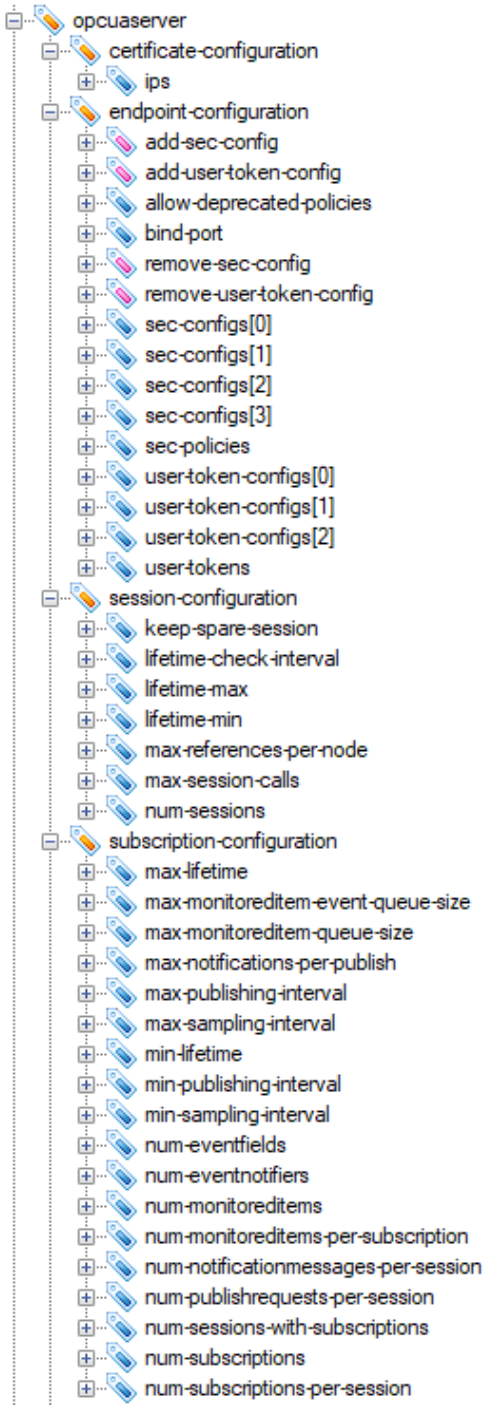

Fig. 16: Server configuration view in the address space of the ctrlX OPC UA Server

5.4.1 Certificate configuration

For the Certificate configuration, go to the Data Layer item *Certificate-configuration*.

The following configuration parameters (Data Layer items) are available:

Data Layer item	Data type	Description	Default value
ips	String	List of IPs separated by commas	

The *ips* field describes a list of IPs (e.g. "192.168.1.1,127.0.0.1”) separated by q comma and written to the "IPAddresses" field when generating the certificate.

The certificate is only newly generated if the certificate (default:"rexroth-opcua-server2048.der") was deleted manually before via the ctrlX WebUI under “Settings → Certificate & Keys → OPC UA Server”.

5.4.2 Endpoint configuration

For the endpoint configuration, go to the Data Layer item *endpoint-configuration*.

The following configuration parameters (Data Layer items) are available:

Data Layer item	Data type	Description	Default value
allow-deprecated-policies	Bool	Allowing the use of outdated security policies for the secure-channel and the user token	false
bind-port	UInt32	port number (valid range 1 - 65535)	4840
sec-configs[n]	sechan-config	Array of security configurations (endpoints as specified for OPC UA)	sec-configs[0] sec-configs[1] sec-configs[2] sec-configs[3]
sec-configs[n].mode-None	Bool	"true” if the message security mode "none" is permitted	[0] => false [1] => false [2] => false [3] => false
sec-configs[n].mode-Sign	Bool	"true” if the message security mode "sign" is permitted	[0] => false [1] => true [2] => true [3] => true
sec-configs[n].mode-SignAndEncrypt	Bool	"true” if the message security modes "sign" and "encrypt" are permitted	[0] => false [1] => true [2] => true [3] => true
sec-configs[n].policyId	UInt32 (enum SecurityPolicy)	Identifier of the policy used	[0] => 0 [1] => 3 [2] => 4 [3] => 5
sec-policies	Byte array	Index array of the security policies for this endpoint	0,1,2,3
user-token-configs[n]	user-token	Array of user identity token	user-token-configs[0] user-token-configs[1] user-token-configs[2]

Data Layer item	Data type	Description	Default value
user-token-configs[n].policyId	UInt32 (enum SecurityPolicy)	Identifier of the policy used	[0] => 0 [1] => 3 [2] => 5
user-token-configs[n].type	UInt32 (enum UserIdentityTokenType)	UserIdentityTokenType type	[0] => 0 [1] => 1 [2] => 1
user-tokens	ByteArray	Index array of the user token types for this endpoint	0,1,2

The default settings (refer to the default values in the table) correspond to the ones shown in the “Endpoints” section.

Enumerations are currently not supported in the data range of the Data Layer. Thus, write the respective Uint32 value for the fields "policyId" and "type" to sec-configs and to user-token-configs.

The Endpoint configuration also allows to provide an unencrypted OPC UA endpoint. An unencrypted connection is only recommended for diagnostic purposes. The unencrypted connection should not be used and the respective OPC UA endpoint should be disabled for the general operation.

Enumeration SecurityPolicy

Name	Value (UInt32)	Description
NONE	0	➥ http://opcfoundation.org/UA/SecurityPolicy#None
BASIC128RSA15	1	➥ http://opcfoundation.org/UA/SecurityPolicy#Basic128Rsa15
BASIC256	2	➥ http://opcfoundation.org/UA/SecurityPolicy#Basic256
BASIC256SHA256	3	➥ http://opcfoundation.org/UA/SecurityPolicy#Basic256Sha256
AES128_SHA256_RSAOAEP	4	➥ http://opcfoundation.org/UA/SecurityPolicy#Aes128_Sha256_RsaOaep
AES256_SHA256_RSAPSS	5	➥ http://opcfoundation.org/UA/SecurityPolicy#Aes256_Sha256_RsaPss

The SecurityPolicies BASIC128RSA15 and BASIC256 are provided due to compatibility reasons. They are not secure and should thus not be used.

UserIdentityTokenType enumeration

Name	Value (UInt32)	Description
ANONYMOUS	0	No token required
USERNAME	1	A username/password token
CERTIFICATE	2	X.509 v3 certificate token
ISSUEDTOKEN	3	Each token created by a authorization service

The server supports an “Anonymous” token type for test purposes only.

The error message "Bad_IdentityTokenInvalid” is always issued when setting up a connection to an “Anonymous” token.

Method add-sec-config

Use the method add-sec-config to add a new security configuration. The added security configuration is attached at the end of the "sec-configs” array.

Method add-user-token-config

Use the method add-user-token-config to add a new UserIdentity configuration. The added security configuration is attached at the end of the "user-token-configs" array.

The input parameters "policyId" and "type" correspond to the fields of the "user-token-configs" structure.

Method remove-sec-config

The remove-sec-config method removes an element from the array of the security configuration "sec-configs".

The input parameter "index" is the index (UInt32) of the array field to be removed.

Method remove-user-token-config

The remove-user-token-config method removes an element from the array of the UserIdentity configuration "user-token-configs".

The input parameter "index" is the index (UInt32) of the array field to be removed.

5.4.3 Session configuration

For the Session configuration, go to the Data Layer item *session-configuration*.

The following configuration parameters (Data Layer items) are available:

Datalayer item	Data type	Description	Default value	Minimum value	Maximum value
keep-spare-session	Bool	If "true", the oldest disconnected session is deleted when num-sessions is reached.	true:	-	-
lifetime-check-interval	UInt32	Interval in ms during which the session lifetime is checked	5000	100	5000
lifetime-max	UInt32	Maximum session lifetime in milliseconds	3600000	360000	3600000
lifetime-min	UInt32	Minimum session lifetime in milliseconds	10000	1000	50000
max-references-per-node	UInt32	Limits the maximum number of references returned in a browse request	100	1	500
max-session-calls	UInt32	Maximum number of service calls (per server; not per session!; related to num_uatcpmsg_ctxts)	250	1	500
num-sessions	UInt32	Maximum number of parallel sessions (per server)	12	1	50

5.4.4 Subscription configuration

For the Subscription configuration, go to the Data Layer item *subscription-configuration*.

The following configuration parameters (Data Layer items) are available:

Datalayer item	Data type	Description	Default value	Minimum value	Maximum value
max-lifetime	UInt32	Maximum interval after which there is the Subscription timeout (milliseconds)	100000	1	500000
max-monitor-editem-event-queue-size	UInt32	Maximum supported number of events in a monitoreditem	100	1	500
max-monitore-ditem-queue-size	UInt32	Maximum supported values of events in a monitoreditem	100	1	500
max-notifica-tions-per-publish	UInt32	Sum of the values and results in a publishresponse	1000	1	5000
max-publishing-interval	UInt32	Maximum supported publishing interval	10000	1	50000
max-sampling-interval	UInt32	Maximum supported sampling interval	10000	1	50000
min-lifetime	UInt32	Minimum interval after which there is the Subscription timeout (milliseconds)	1000	1	2000
min-publishing-interval	UInt32	Minimum supported publishing interval	10	1	2000
min-sampling-interval	UInt32	Minimum supported sampling interval	10	1	2000
num-eventfields	UInt32	Number of eventfields	200	1	500
num-eventnoti-fiers	UInt32	Number of eventnotifiers and eventsources	20	1	50
num-monitoredi-tems	UInt32	Total number of available moni-toreditems	5000	1	5000
num-monitore-ditems-per-sub-scription	UInt32	Maximum number of monitoredi-tems in a Subscription	500	1	2000
num-notification-messages-per-session	UInt32	Retransmission Queue, has to be at least twice the num_publishre-quests_per_session	100	1	200
num-publishre-quests-per-ses-sion	UInt32	Maximum number of publishre-quests in one session in the waiting queue	10	1	150
num-sessions-with-subscrip-tions	UInt32	Only this number of sessions can obtain a Subscription	10	1	150
num-subscrip-tions	UInt32	Total number of available Sub-scriptions	50	1	150
num-subscrip-tions-per-session	UInt32	Maximum number of Subscrip-tions in one session	10	1	150

5.5 Web interface

From 1.12.0, a web interface to access status and configuration data is provided with the app upon delivery.

After installing the ctrlX OPC UA Server app, this apps integrates itself automatically into the web interface of the control (see Fig. 17).

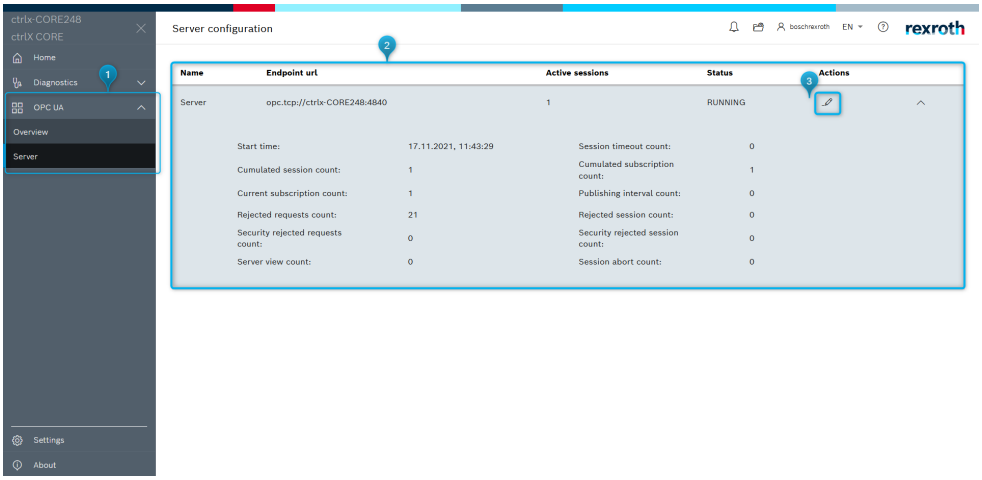

Fig. 17: Web interface of the ctrlX OPC UA Server app

The web interface of the OPC UA app is divided into the following sections:

- **① side navigation**:
  Entry point to the OPC UA-specific settings
- **② window OPC UA Server configuration**:
  Representation of current server data, e.g. the number of current sessions
- **③ button** 
  Opens a sidebar to configure the ctrlX OPC UA Server.

For basic configurations of the ctrlX OPC UA Server, open the sidebar Setup Server using  (see Fig. 18).

A changed configuration is applied upon the next app restart.

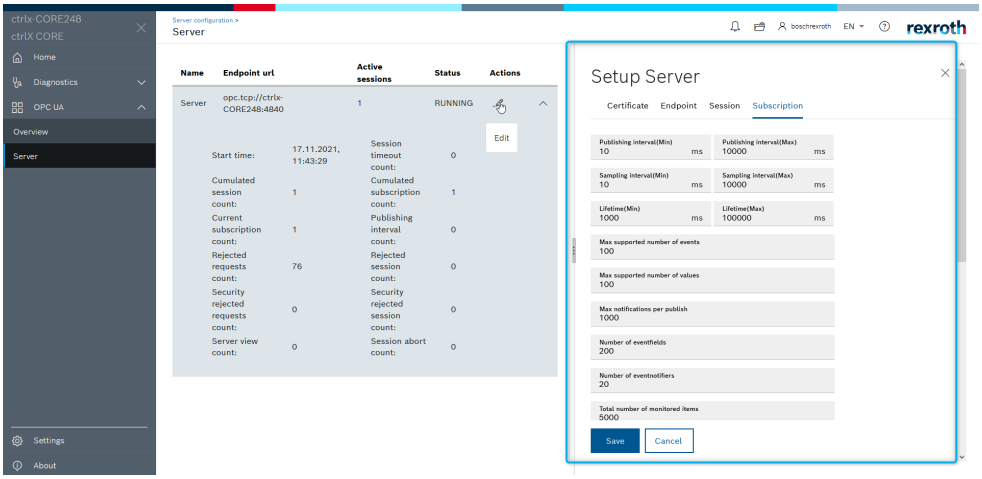

Fig. 18: OPC UA Server - Sidebar when opening 

6 Related documentation

6.1 Overview

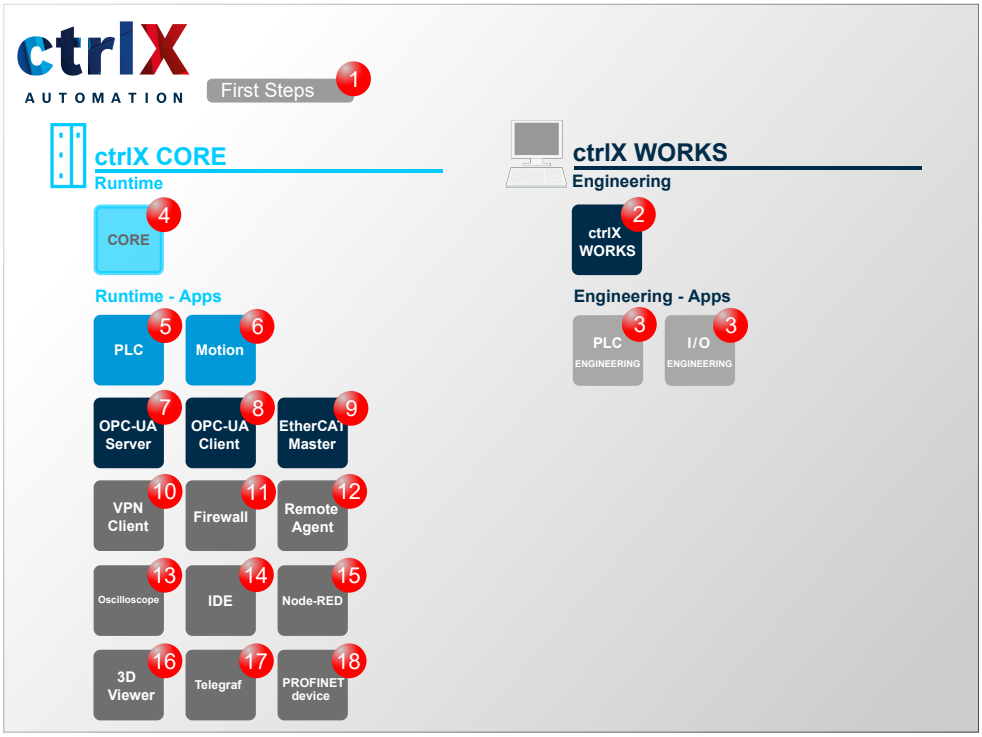

Fig. 19: Overview on further documentations

6.2 ctrlX AUTOMATION

No.	Documentation
1	**ctrlX WORKS First Steps** Quick Start Guide ➦ Web documentation link Ordering information: • DOK-XWORKS-F*STEP*****-QURS-EN-P • R911403760

6.3 ctrlX WORKS

No.	Documentation
2	**ctrlX WORKS Basic System** Application Manual ➥ Web documentation link Ordering information: • DOK-XWORKS-**********-APRS-EN-P • R911403761
3	**ctrlX PLC Engineering - PLC Programming System** Application Manual ➥ Web documentation link Ordering information: • DOK-XPLC**-ENGINEERING-APRS-EN-P • R911403764
3	**ctrlX PLC Engineering - PLC Libraries** Reference ➥ Web documentation link Ordering information: • DOK-XPLC**-LIBRARY****-RERS-EN-P • R911403766

6.4 ctrlX CORE

No.	Documentation
4	**ctrlX CORE - Runtime** Application Manual ➥ Web documentation link Ordering information: • DOK-XCORE*-BASE*******-APRS-EN-P • R911403768
	ctrlX CORE - Diagnostics Reference ➥ Web documentation link Ordering information: • DOK-XCORE*-DIAG*******-RERS-EN-P • R911403770

6.5 ctrlX CORE apps

No.	Documentation
5	**PLC App - PLC Runtime Environment for ctrlX CORE** Application Manual ➥ Web documentation link Ordering information: • DOK-XCORE*-PLC********-APRS-EN-P • R911403787

No.	Documentation
6	**Motion App - Motion Runtime Environment for ctrlX CORE** Application Manual ➦ Web documentation link Ordering information: • DOK-XCORE*-MOTION*****-APRS-EN-P • R911403791
7	**OPC UA Server App - OPC UA Server for ctrlX CORE** Application Manual ➦ Web documentation link Ordering information: • DOK-XCORE*-OPCUA*SERV*-APRS-EN-P • R911403778
8	**OPC UA Client App - OPC UA Client for ctrlX CORE** Application Manual ➦ Web documentation link Ordering information: • DOK-XCORE*-OPCUA*CLIEN-APRS-EN-P • R911403781
9	**EtherCAT Master App - EtherCAT master for ctrlX CORE** Application Manual ➦ Web documentation link Ordering information: • DOK-XCORE*-ETHERCAT***-APRS-EN-P • R911403773
10	**VPN Client App - Remote Support Software for ctrlX CORE** Application Manual ➦ Web documentation link Ordering information: • DOK-XCORE*-VPN********-APRS-EN-P • R911403775
11	**Firewall App - Security Functions for ctrlX CORE** Application Manual ➦ Web documentation link Ordering information: • DOK-XCORE*-FIREWALL***-APRS-EN-P • R911403783
12	**Remote Agent App - ctrlX Device Portal Connection for ctrlX Devices** Application Manual ➦ Web documentation link Ordering information: • DOK-XCORE*-REMOTE*AG**-APRS-EN-P • R911403785

No.	Documentation
13	**Oscilloscope App - Oscilloscope Function for ctrlX Devices** Application Manual ➦ Web documentation link Ordering information: • DOK-XCORE*-OSCI*******-APRS-EN-P • R911409806
14	**IDE App - Integrated Development Environment** Application Manual ➦ Web documentation link Ordering information: • DOK-XCORE*-IDE********-APRS-EN-P • R911410625
15	**Node RED App - Graphic Programming for ctrlX CORE** Application Manual ➦ Web documentation link Ordering information: • DOK-XCORE*-NODE*RED***-APRS-EN-P • R911403789
16	**3D Viewer App - Browser-based 3D Kinematic Simulation for ctrlX CORE** Application Manual ➦ Web documentation link Ordering information: • DOK-XCORE*-3D*VIEWER**-APRS-EN-P • R911416124
17	**Telegraf App - Server Agent for Collecting Data in the Data Layer** Application Manual ➦ Web documentation link Ordering information: • DOK-XCORE*-TELEGRAF***-AP01-EN-P • R911416836
18	**PROFINET device App - PROFINET device for ctrlX CORE** Application Manual ➦ Web documentation link Bestellinformationen: • DOK-XCORE*-PROFINET***-AP01-EN-P • R911417857

7 Service and support

Our worldwide service network provides an optimized and efficient support. Our experts provide you with advice and assistance. You can contact us **24/7**.

Service Germany

Our technology-oriented Competence Center in Lohr, Germany, is responsible for all your service-related queries for electric drive and controls.

Contact the **Service Hotline** and **Service Helpdesk** under:

Phone:	**+49 9352 40 5060**
Fax:	**+49 9352 18 4941**
Email:	➦service.svc@boschrexroth.de
Internet:	➦http://www.boschrexroth.com

Additional information on service, repair (e.g. delivery addresses) and training can be found on our internet sites.

Service worldwide

Outside Germany, please contact your local service office first. For hotline numbers, refer to the sales office addresses on the internet.

Preparing information

To be able to help you more quickly and efficiently, please have the following information ready:

- Detailed description of malfunction and circumstances
- Type plate specifications of the affected products, in particular type codes and serial numbers
- Your contact data (phone and fax number as well as your e-mail address)

8 Index

rexroth
A Bosch Company

Bosch Rexroth AG
Bgm.-Dr.-Nebel-Str. 2
97816 Lohr a.Main
Germany
Tel. +49 9352 18 0
Fax +49 9352 18 8400
www.boschrexroth.com/electrics

R911403778