CODESYS OPC UA Server SL

An additional option for CODESYS runtime systems to publish variables via the OPC UA protocol. For advanced use cases the linkage of an information model to the PLC application is possible.

Product description

The OPC UA Server exposes specified variables of a CODESYS project to the OPC UA address space. Clients can read, write and monitor the values of the PLC. Custom information models can be easily imported and linked to the PLC application. This also enables the execution of PLC methods by clients.

Also see [CODESYS Online Help](https://content.helpme-codesys.com/en/CODESYS%20Communication/_cds_runtime_opc_ua_server.html).

Certified compliance

OPC Foundation Certified for Compliance logo is a trademark of the OPC Foundation and may be used only by written permission of the OPC Foundation. Any unauthorized use of the Certified for Compliance logo is prohibited.

OPC Foundation Certified for Compliance logo indicates that this product has been tested by an independent certification lab and certified to be compliant with the following OPC UA Profiles which are part of the OPC UA Specifications:

- Micro Embedded Device 2017 Server Profile
- Method Server Facet
- SecurityPolicy [B] – Basic256Sha256
- SecurityPolicy [A] - Aes128-Sha256-RsaOaep
- SecurityPolicy - Aes256-Sha256-RsaPss
- User Token – Anonymous Server Facet

- User Token - User Name Password Server Facet

Supported features

The OPC UA Server supports the following features:

- Browsing of data types and variables
- Standard read/write services
- Notification for value changes (subscription and monitored item services)
- No restriction in the number of sessions, monitored items, and subscriptions (the number depends on the performance of the respective platform)
- Support of events
- Support of complete access to structures
- Encrypted communication with an OPC UA Client
- Support of multitasking
- Support of OPC UA methods
- Support of Alarms&Conditons

Supported profiles: Currently the OPC UA server supports the “Micro Embedded Device Server Profile”. This server profile allows reading, writing, and subscribing of items.

Supported information models: OPC UA allows defining different data types. The combination of customer defined data types, object types and reference types allows defining your own information model. An information model describes how the data should be exposed to the address space.

- PLCopen information model
- User-defined information models (companion specifications)

Also see [CODESYS Online Help](https://content.helpme-codesys.com/en/CODESYS%20Communication/_cds_using_opc_ua_information_models.html).

Security:

- signed and encrypted communication
- User management

SecurityProfiles:

- None
- Basic256Sha256 (Sign, Sign_and_Encrypt)
- Aes128_Sha256_RsaOaep
- Aes256_Sha256_RsaPss

User token policy:

- Anonymouse
- Username

Supported profiles

The CODESYS OPC UA Server supports the following profiles. Please note that the mapping of the Alarms&Conditions profile to the CODESYS Alarm Configuration is not yet compliant to the specification.

UA Features	Profiles	Link
Core	Micro Embedded Device Server Profile	http://opcfoundation.org/UA-Profile/Server/MicroEmbeddedDevice
	UA-TCP UA-SC UA-Binary	http://opcfoundation.org/UA-Profile/Transport/uatcp-uasc-uabinary
Event Acess	Standard Event Subscription Server	http://opcfoundation.org/UA-Profile/Server/StandardEventSubscription
Methods	Method Server Facet	http://opcfoundation.org/UA-Profile/Server/Methods
Alarms&Conditions	A & C Base Condition Server Facet	http://opcfoundation.org/UA-Profile/Server/ACBaseCondition
	A & C Refresh2 Server Facet	http://opcfoundation.org/UA-Profile/Server/ACRefresh2
	A & C Enable Server Facet	http://opcfoundation.org/UA-Profile/Server/ACEnable
	A & C Acknowledgeable Alarm Server Facet	http://opcfoundation.org/UA-Profile/Server/ACAckAlarm
	A & C Alarm Server Facet	http://opcfoundation.org/UA-Profile/Server/ACAlarm
Historical Access	not yet supported	
Redundancy	not yet supported	
Security	User Token – Anonymous Facet	http://opcfoundation.org/UA-Profile/Security/UserToken/Anonymous
	User Token – User Name Password Client Facet	http://opcfoundation.org/UA-Profile/Security/UserToken/Client/UserNamePassword
	None	http://opcfoundation.org/UA/SecurityPolicy#None
	SecurityPolicy [B] – Basic256Sha256	http://opcfoundation.org/UA/SecurityPolicy#Basic256Sha256
	Aes128-Sha256-RsaOaep	http://opcfoundation.org/UA/SecurityPolicy#Aes128_Sha256_RsaOaep
	Aes256-Sha256-RsaPss	http://opcfoundation.org/UA/SecurityPolicy#Aes256_Sha256_RsaPss

General information

Supplier:

CODESYS GmbH
Memminger Strasse 151
87439 Kempten
Germany

Support:

Technical support is not included with this product. To receive technical support, please purchase a CODESYS Support Ticket.

https://support.codesys.com

Item:

CODESYS OPC UA Server SL

Item number:

2302000041

Sales / Source of supply:

CODESYS Store
https://store.codesys.com

Included in delivery:

- License key
- License agreement

System requirements and restrictions

Programming System	CODESYS Development System V3.5.17.0 or higher
Runtime System	CODESYS Control V3.5.17.0 or higher
Supported Platforms/ Devices	CODESYS SoftPLC systems Note: Use the tool “Device Reader” to find out the supported features of your device (free of charge component of CODESYS Development System).
Additional Requirements	TCP/IP stack Real-time watch
Restrictions	-
Licensing	

	Single Device License: The license can be used on the target device/PLC on which the CODESYS Runtime System is installed. Licenses are activated on a software-based license container (soft container), which is permanently connected to the controller. Alternatively the license can be stored on a CODESYS Key (USB-Dongle). By replugging the CODESYS Key, the license can be used on any other controller. Note: In demo mode, the software runs for two hours without a license. After that, a manual restart is required.
Required Accessories	Optional: CODESYS Key

Note: Technical specifications are subject to change. Errors and omissions excepted. The content of the current online version of this document applies.

Creation date: 2023-06-05