SD02040D/06/EN/02.19
71446702
2019-09-01

Special Documentation
Proline Promass 500 HART

OPC-UA Server application package
for IIoT and SCADA applications

HART COMMUNICATION PROTOCOL

Endress+Hauser
People for Process Automation

Table of contents

1 About this document

1.1 Document function

This manual is Special Documentation; it does not replace the Operating Instructions pertaining to the device. It serves as a reference for using the optional "OPC-UA Server" application package.

1.2 Target audience

The document is aimed at specialists who work with the device over the entire life cycle and perform specific configurations for IIoT and SCADA applications.

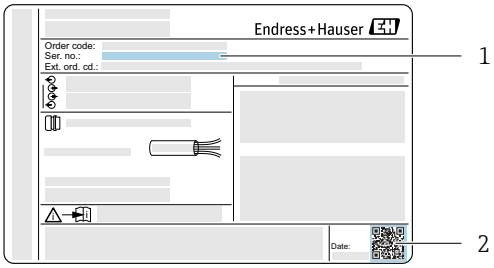
1.3 Using this document

1.3.1 Information on the document structure

This Special Documentation contains a range of information, including:
- Device-specific IT security
- Product features and availability
- Device operating options for accessing the OPC-UA parameters
- Integration of the device into a plant network
- Application examples and Heartbeat Verification
- OPC-UA information model

1.3.2 Device documentation

The relevant Operating Instructions, the description of the device parameters and all other technical documentation for the device are available via:
- Internet: *W@M Device Viewer* (www.endress.com/deviceviewer):
  Enter the device serial number indicated on the transmitter nameplate.
- Smart phone/tablet: *Endress+Hauser Operations App* (App Store or Google Play):
  Enter the device serial number indicated on the transmitter nameplate or scan the 2-D matrix code (QR code) on the nameplate.



A0034947

1 Example of a transmitter nameplate

1 Serial number (ser. no.)
2 2-D matrix code (QR code)

Technical documentation can also be downloaded from the Download Area of the Endress+Hauser Web site: www.endress.com → Download.

However this technical documentation applies to a particular instrument family and is not assigned to a specific measuring device.

1.4 Symbols used

1.4.1 Safety symbols

DANGER
This symbol alerts you to a dangerous situation. Failure to avoid this situation will result in serious or fatal injury.

WARNING
This symbol alerts you to a dangerous situation. Failure to avoid this situation can result in serious or fatal injury.

CAUTION
This symbol alerts you to a dangerous situation. Failure to avoid this situation can result in minor or medium injury.

NOTICE
This symbol contains information on procedures and other facts which do not result in personal injury.

1.4.2 Symbols for certain types of information

Symbol	Meaning
✓	**Permitted** Indicates procedures, processes or actions that are allowed.
✗	**Forbidden** Indicates procedures, processes or actions that are forbidden.
i	**Tip** Indicates additional information.
	Reference to documentation
	Reference to page
	Reference to graphic
▶	Notice or individual step to be observed
1., 2., 3....	Series of steps
↳	Result of a step

1.4.3 Symbols in graphics

Symbol	Meaning
1, 2, 3,...	Item numbers
1., 2., 3....	Series of steps

1.4.4 Electrical symbols

Symbol	Meaning
⏚	**Ground connection** A grounded terminal which, as far as the operator is concerned, is grounded via a grounding system.
⏚	**Protective earth (PE)** Ground terminals that must be connected to ground prior to establishing any other connections. The ground terminals are located on the interior and exterior of the device: ▪ Interior ground terminal: protective earth is connected to the mains supply. ▪ Exterior ground terminal: device is connected to the plant grounding system.

1.4.5 Communication symbols

Symbol	Meaning
	Wireless Local Area Network (WLAN) Communication via a wireless, local network.

2 Basic safety instructions

2.1 Requirements for personnel

Personnel involved in installation, commissioning, diagnostics and maintenance must meet the following requirements:
- Trained, qualified specialists must have a relevant qualification for this specific function and task
- Are authorized by the plant owner/operator
- Are familiar with federal/national regulations
- Before starting work, read and understand the instructions in the manual and supplementary documentation as well as the certificates (depending on the application)
- Follow instructions and comply with basic conditions

Operating personnel must meet the following requirements:
- Be instructed and authorized by the plant operator with regard to the requirements of the task
- Follow the instructions in this manual

2.2 Designated use

The designated use of the measuring device is described in the Operating Instructions pertaining to the device.

2.3 Occupational safety

For work on and with the device:
- Wear the required personal protective equipment according to federal/national regulations.

If working on and with the device with wet hands:
- It is recommended to wear gloves on account of the higher risk of electric shock.

2.4 Operational safety

Risk of injury!
- Operate the device in proper technical condition and fail-safe condition only.
- The operator is responsible for interference-free operation of the device.

Modifications to the device

Unauthorized modifications to the device are not permitted and can lead to unforeseeable dangers.
- If, despite this, modifications are required, consult with Endress+Hauser.

2.5 Product safety

This device is designed in accordance with good engineering practice to meet state-of-the-art safety requirements, has been tested, and left the factory in a condition in which it is safe to operate.

It meets general safety standards and legal requirements. It also complies with the EC directives listed in the device-specific EC Declaration of Conformity. Endress+Hauser confirms this by affixing the CE mark to the device.

2.6 IT security

Our warranty is valid only if the device is installed and used as described in the Operating Instructions. The device is equipped with security mechanisms to protect it against any inadvertent changes to the settings.

IT security measures, which provide additional protection for the device and associated data transfer, must be implemented by the operators themselves in line with their security standards.

2.7 Device-specific IT security

The device offers a range of specific functions to support protective measures on the operator's side. These functions can be configured by the user and guarantee greater in-operation safety if used correctly. An overview of the most important functions is provided in the following section.

Function/interface	Factory setting	Recommendation
Write protection via hardware write protection switch → 🗎 8	Not enabled.	On an individual basis following risk assessment.
Access code (also applies for Web server login or FieldCare connection) → 🗎 9	Not enabled (0000).	Assign a customized access code during commissioning.
WLAN (order option in display module)	Enabled.	On an individual basis following risk assessment.
WLAN security mode	Enabled (WPA2-PSK)	Do not change.
WLAN passphrase (password) → 🗎 9	Serial number	Assign an individual WLAN passphrase during commissioning.
WLAN mode	Access Point	On an individual basis following risk assessment.
Web server→ 🗎 9	Enabled.	On an individual basis following risk assessment.
OPC-UA → 🗎 9	–	On an individual basis following risk assessment.
CDI-RJ45 service interface → 🗎 10	–	On an individual basis following risk assessment.

2.7.1 Protecting access via hardware write protection

Write access to the device parameters via the local display, Web browser or operating tool (e.g. FieldCare, DeviceCare) can be disabled via a write protection switch (DIP switch on the motherboard). When hardware write protection is enabled, only read access to the parameters is possible.

Hardware write protection is disabled when the device is delivered.

2.7.2 Protecting access via a password

Different passwords are available to protect write access to the device parameters or access to the device via the WLAN interface.

- User-specific access code
  Protect write access to the device parameters via the local display, Web browser or operating tool (e.g. FieldCare, DeviceCare). Access authorization is clearly regulated through the use of a user-specific access code.
- WLAN passphrase
  The network key protects a connection between an operating unit (e.g. notebook or tablet) and the device via the WLAN interface which can be ordered as an option.
- Infrastructure mode
  When the device is operated in infrastructure mode, the WLAN passphrase corresponds to the WLAN passphrase configured on the operator side.

User-specific access code

Write access to the device parameters via the local display, Web browser or operating tool (e.g. FieldCare, DeviceCare) can be protected by the modifiable, user-specific access code.

When the device is delivered, the device does not have an access code and is equivalent to *0000* (open).

WLAN passphrase: Operation as WLAN access point

A connection between an operating unit (e.g. notebook or tablet) and the device via the WLAN interface, which can be ordered as an optional extra, is protected by the network key. The WLAN authentication of the network key complies with the IEEE 802.11 standard.

When the device is delivered, the network key is pre-defined depending on the device. It can be changed via the **WLAN settings** submenu in the **WLAN passphrase** parameter.

Infrastructure mode

A connection between the device and WLAN access point is protected by means of an SSID and passphrase on the system side. Please contact the relevant system administrator for access.

General notes on the use of passwords

- The access code and network key supplied with the device should be changed during commissioning.
- Follow the general rules for generating a secure password when defining and managing the access code or network key.
- The user is responsible for the management and careful handling of the access code and network key.

2.7.3 Access via Web server

The Web server is enabled when the device is delivered. The Web server can be disabled if necessary (e.g. after commissioning) via the **Web server functionality** parameter.

The device and status information can be hidden on the login page. This prevents unauthorized access to the information.

For detailed information on device parameters, see:
The "Description of Device Parameters" document → 📄 4

2.7.4 Access via OPC-UA

The following Security Modes are supported as per the OPC UA Specification (IEC 62541):
- None
- Basic128Rsa15 – signed
- Basic128Rsa15 – signed and encrypted

Username and password

Authentication is via a username and login password.

The fixed username defined for OPC UA is "Maintenance". It cannot be changed. Access is only possible in the maintenance user role.

The password corresponds to the login password. A change in the login password affects the user.

2.7.5 Access via service interface (CDI-RJ45)

The device can be connected to a network via the service interface (CDI-RJ45). Device-specific functions guarantee the secure operation of the device in a network.

The use of relevant industrial standards and guidelines that have been defined by national and international safety committees, such as IEC/ISA62443 or the IEEE, is recommended. This includes organizational security measures such as the assignment of access authorization as well as technical measures such as network segmentation.

Transmitters with an Ex de approval may not be connected via the service interface (CDI-RJ45)!

Order code for "Approval transmitter + sensor", options (Ex de): BA, BB, C1, C2, GA, GB, MA, MB, NA, NB

3 Product features and availability

3.1 Product features

The "OPC-UA Server" application package allows the device to communicate with an OPC-UA client and be integrated into Industrial Internet of Things (IIoT) and Supervisory Control And Data Acquisition (SCADA) applications.

The device can be integrated via:
- The WLAN interface and WLAN access point.
- The service interface (CDI-RJ45) and Ethernet network/Ethernet switch.

In addition to the measured values, device status information is also displayed, allowing users to monitor the status of the device. The device supports the *Data Access* OPC-UA operating mode.

A device that has a WLAN interface (can be ordered as an option) is required for the WLAN connection: order code for "Display; operation", option **G** "4-line, illuminated; touch control + WLAN".

3.2 Availability

The OPC-UA server is integrated in the device. The "OPC-UA Server" application package for using the OPC-UA server can either be ordered directly with the device or subsequently.

The "OPC-UA Server" application package can be ordered via:
Order option for "Application package", option **EL** "OPC-UA Server"

The "OPC-UA Server" application package is available as follows:
- If the application package was ordered with the device:
  the package is available directly when the device is commissioned.
- If the application package was ordered subsequently:
  the package is available once it has been enabled in the **Activate SW option** parameter (the service code must be entered).

No special measures are required to put the OPC-UA Server into operation.

To display all the application packages available for the device: **Software option overview** parameter
If the "OPC-UA Server" application package is not listed in the **Software option overview** parameter, the device firmware needs to be updated: please contact your Endress+Hauser service organization.

Detailed information on the device parameters:
- "Description of Device Parameters" document → 📄 4
- Detailed information on the OPC-UA parameters of the device → 📄 30.

4 System integration

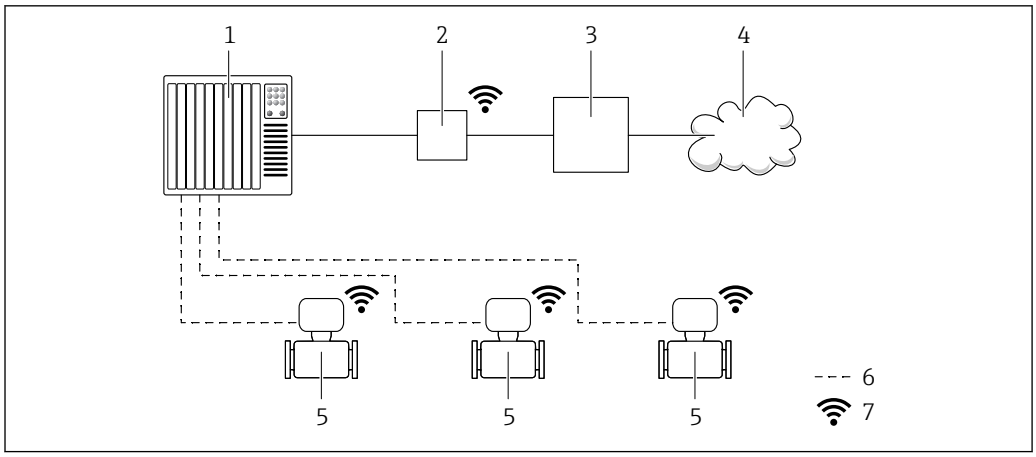
The device is integrated into a plant network for permanent access to measured values and status information for IIoT and SCADA applications. This can be done in either of two ways:

- Via WLAN by means of the WLAN interface/access point: the device is connected to an access point via WLAN by means of the WLAN interface and integrated into the plant network → 12.
- Via Ethernet network/switch by means of the service interface (CDI-RJ45): the device is connected to an Ethernet network via the service interface (CDI-RJ45) and integrated into the plant network via an Ethernet switch → 13.

Measured values are displayed and the device is accessed independently of the integration into a plant network described here. A separate connection to the automation system is established via the inputs and outputs of the device for this purpose.

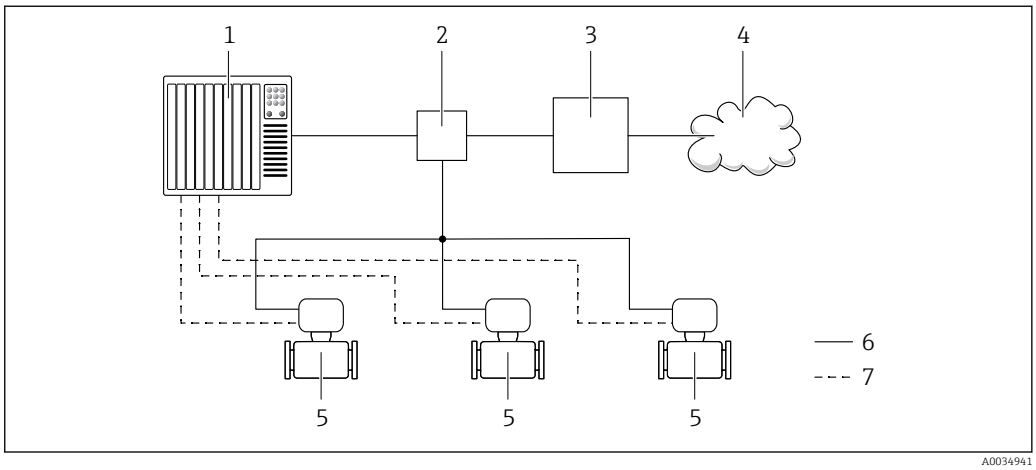
4.1 By WLAN via the WLAN interface and access point

The optional WLAN interface is available on the following device version:
Order code for "Display; operation", option **G** "4-line, illuminated, graphic display; touch control + WLAN"



1 *Automation system, e.g. Simatic S7 (Siemens)*
2 *Access point*
3 *Edge Gateway*
4 *Cloud*
5 *Measuring device*
6 *Measured values and access to the device via inputs and outputs*
7 *Optional WLAN interface*

4.2 Via Ethernet network/switch by means of the service interface (CDI-RJ45)



1 *Automation system, e.g. Simatic S7 (Siemens)*
2 *Ethernet switch*
3 *Edge Gateway*
4 *Cloud*
5 *Measuring device*
6 *Ethernet network*
7 *Measured values and access to the device via inputs and outputs*

4.2.1 Connecting the device with the Ethernet network: Proline 500 – digital

The device is connected on an Ethernet network by an Ethernet switch.

The connection to the Ethernet network is via an Ethernet connector on the service interface (CDI-RJ45) of the device.

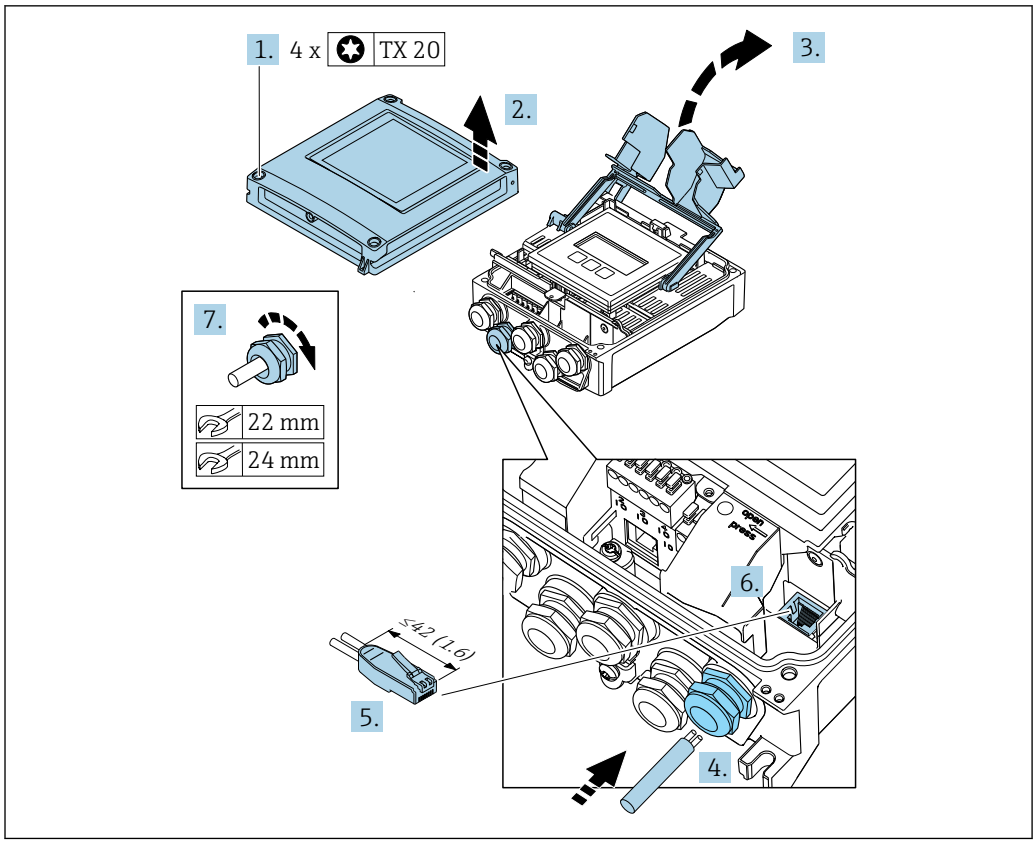
NOTICE

Electrical safety is compromised by an incorrect connection!

- Have electrical connection work carried out by appropriately trained specialists only.
- Observe applicable federal/national installation codes and regulations.
- Comply with local workplace safety regulations.
- Always connect the protective ground cable ⏚ before connecting additional cables.
- If using in potentially explosive atmospheres, observe the information in the device-specific Ex documentation.

An adapter for RJ45 and the M12 connector is optionally available:
Order code for "Accessories", option **NB**: "Adapter RJ45 M12 (service interface)"

The adapter connects the service interface (CDI-RJ45) to an M12 connector mounted in the cable entry. Therefore the connection to the service interface can be established via an M12 connector without opening the device.



1. Loosen the 4 fixing screws on the housing cover.
2. Open the housing cover.
3. Fold open the terminal cover.
4. Push the cable through the cable entry . To ensure tight sealing, do not remove the sealing ring from the cable entry.
5. Strip the cable and cable ends and connect to the RJ45 connector.
6. Plug the RJ45 connector into the service interface (CDI-RJ45).
7. Firmly tighten the cable glands.
8. Close the terminal cover.
9. Close the housing cover.

WARNING

Housing degree of protection may be voided due to insufficient sealing of the housing.

- Screw in the screw without using any lubricant.

WARNING

Excessive tightening torque applied to the fixing screws!

Risk of damaging the plastic transmitter.

- Tighten the fixing screws as per the tightening torque: 2 Nm (1.5 lbf ft)

10. Tighten the 4 fixing screws on the housing cover.

4.2.2 Connecting the device with the Ethernet network: Proline 500

The device is connected on an Ethernet network by an Ethernet switch.

The connection to the Ethernet network is via an Ethernet connector on the service interface (CDI-RJ45) of the device.

NOTICE

Electrical safety is compromised by an incorrect connection!

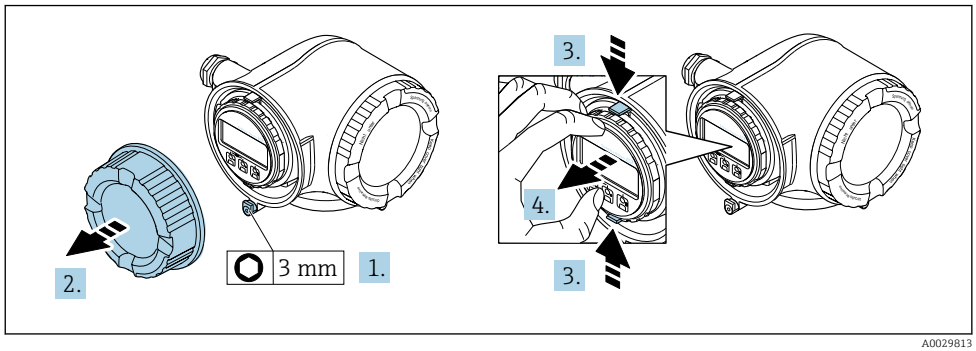
- Have electrical connection work carried out by appropriately trained specialists only.
- Observe applicable federal/national installation codes and regulations.
- Comply with local workplace safety regulations.
- Always connect the protective ground cable ⏚ before connecting additional cables.
- If using in potentially explosive atmospheres, observe the information in the device-specific Ex documentation.

An adapter for RJ45 and the M12 connector is optionally available:
Order code for "Accessories", option **NB**: "Adapter RJ45 M12 (service interface)"

The adapter connects the service interface (CDI-RJ45) to an M12 connector mounted in the cable entry. Therefore the connection to the service interface can be established via an M12 connector without opening the device.

Note the following when connecting without an adapter:
- Recommended cable: CAT 5e, CAT 6 or CAT 7, with shielded connector
- Maximum cable thickness: 6 mm
- Length of connector including anti-bend protection: 42 mm
- Bending radius: 5 x cable thickness

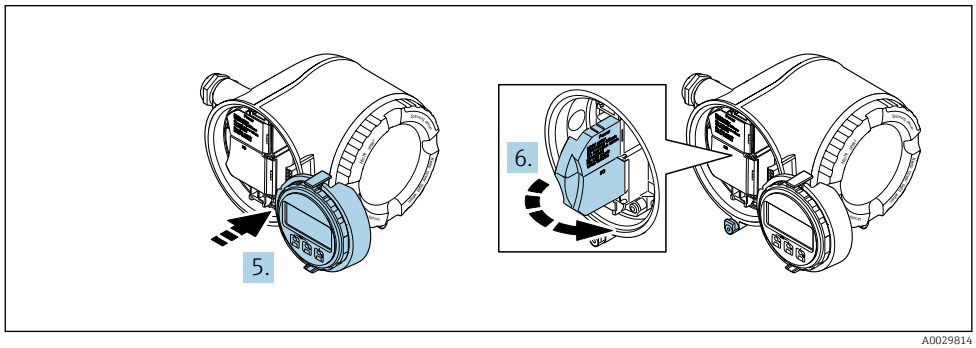
1.



A0029813

Loosen the securing clamp of the connection compartment cover.

2. Unscrew the connection compartment cover.
3. Squeeze the tabs of the display module holder together.
4. Remove the display module holder.
5.

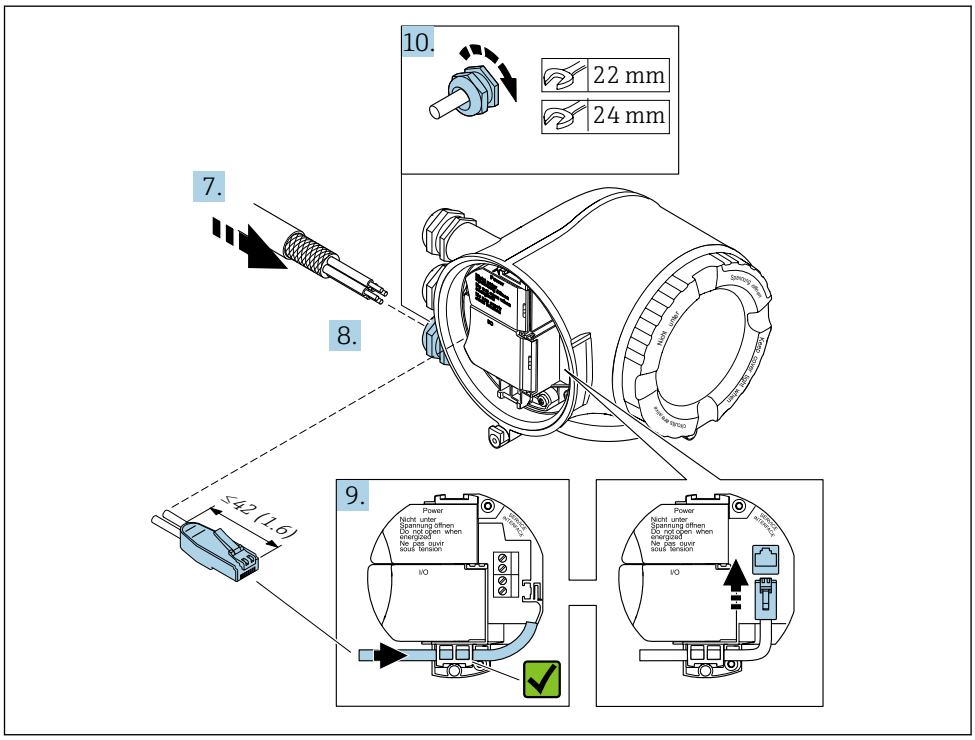


A0029814

Attach the holder to the edge of the electronics compartment.

6. Open the terminal cover.

7.



A0034945

Push the cable through the cable entry . To ensure tight sealing, do not remove the sealing ring from the cable entry.

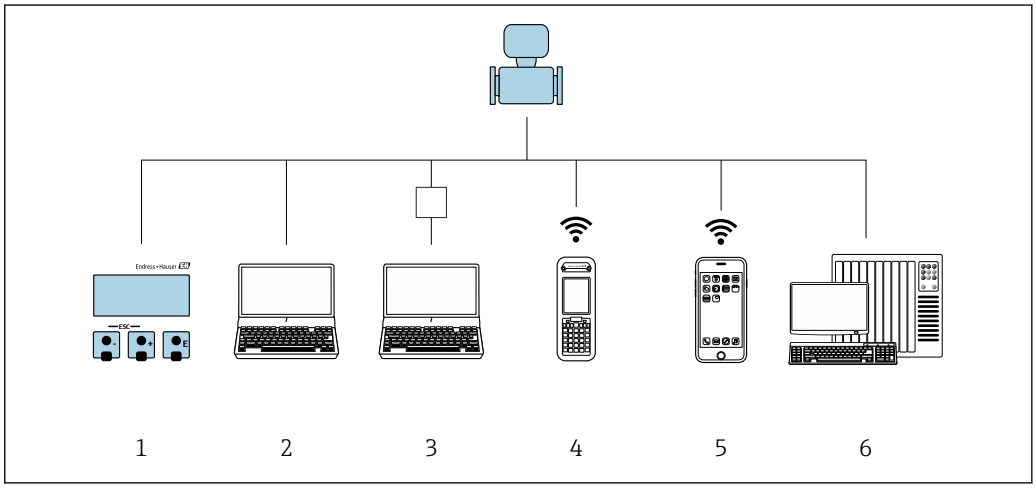
8. Strip the cable and cable ends and connect to the RJ45 connector.
9. Plug the RJ45 connector into the service interface (CDI-RJ45).
10. Firmly tighten the cable glands.
11. Fit the display module holder in the electronics compartment.
12. Screw on the connection compartment cover.
13. Secure the securing clamp of the connection compartment cover.
    ↳ This concludes the connection procedure.

5 Commissioning

The OPC-UA parameters and the WLAN settings of the device must be configured before the device is integrated into an IIoT or SCADA application of a plant network. Only then can a connection be established between the OPC-UA client and the device → 18.

5.1 Accessing device parameters

The device parameters can be accessed via one of the following interfaces:
- Display module – operation via local device operation.
- WLAN interface – operation via the Web server integrated in the device.
  Prerequisite: The device has the optional WLAN interface.
- Service interface (CDI-RJ45)– operation via the Web server integrated in the device.
  Prerequisite: The device is **not** integrated into an IIoT or SCADA application via an Ethernet network. In this case, the service interface (CDI-RJ45) is used for the connection to the Ethernet switch.



2 Overview of the operating options

1 *Local operation via display module*
2 *Computer with Web browser (e.g. Internet Explorer) or with operating tool (e.g. FieldCare, DeviceCare, AMS Device Manager, SIMATIC PDM) via service interface (RJ-45) or WLAN interface of the device*
3 *Computer with Web browser (e.g. Internet Explorer) or with operating tool (e.g. FieldCare, DeviceCare, AMS Device Manager, SIMATIC PDM) via Ethernet switch if the device is integrated into an Ethernet network*
4 *Field Xpert SFX350 or SFX370 via WLAN interface*
5 *Mobile handheld terminal via WLAN interface*
6 *Control system (e.g. PLC)*

For detailed information on the operation of the device:
Operating Instructions for the measuring device → 4.

5.2 Configuring the device parameters

The following settings must be made in the device parameters to use the device in an IIoT or SCADA application of a plant network:

1. Activate the OPC-UA function → 🗎 18.
2. Select the security policy → 🗎 18.
3. Upload the security certificates to the device → 🗎 19.
4. If integrating via WLAN: change the WLAN mode to "WLAN client" → 🗎 20.

Overview of all the OPC-UA parameters → 🗎 30.

5.2.1 Activating the OPC-UA function

- **Activate OPC-UA function** parameter: activate the OPC-UA function (yes)
  - ↳ The device can be integrated into an IIoT or SCADA application of a plant network.

Navigation
"Expert" menu → Communication → OPC-UA configuration → Activate OPC-UA function

Parameter overview with brief description

Parameter	Description	Selection	Factory setting
Activate OPC-UA function	Activate the OPC-UA function.	▪ No ▪ Yes	No

5.2.2 Selecting the security policy

- **Security policy** parameter: activate the OPC-UA functionality (yes)
  - ↳ The device can be integrated into an IIoT or SCADA application of a plant network.

Navigation
"Expert" menu → Communication → OPC-UA configuration → OPC-UA security → Security policy

Parameter overview with brief description

Parameter	Description	Selection	Factory setting
Security policy	Select the security policy.	▪ None ▪ Signed Basic128Rsa15 ▪ Signed and encrypted Basic128Rsa15	None

Description of the security policies

The security policies for communication with the OPC-UA server are defined in the **Security policy** parameter.

- **None** option:
  Every OPC-UA client can establish unencrypted communication with the OPC-UA servers.
- **Signed Basic128Rsa15** option:
  Only an authorized OPC-UA client may establish unencrypted, yet tamper-proof, communication (as per Basic128Rsa15) with the OPC-UA servers.
- **Signed and encrypted Basic128Rsa15** option:
  Only an authorized OPC-UA client may establish encrypted and tamper-proof communication (as per Basic128Rsa15) with the OPC-UA servers.

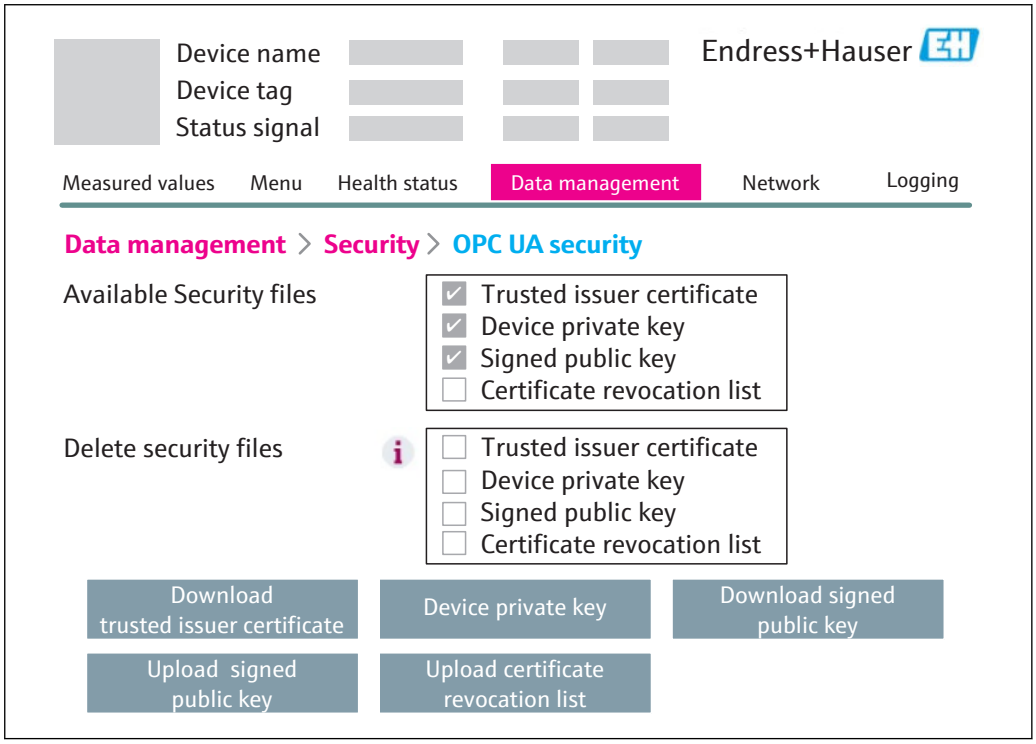
5.2.3 Uploading the security certificates to the device

Different security certificates and a certificate revocation list must be provided in the device, depending on the selected security policy.

In the Web server, the function Data management → Security → OPC UA security lists the security certificates which the device currently has and indicates whether a certificate revocation list is available. In this function it is also possible to upload necessary security certificates and the certificate revocation list to the device or remove them from the device.

- Data management → Security → OPC UA security: upload the necessary security certificates and a certificate revocation list to the device.
  - ↳ The device's OPC server can be identified by the OPC-UA client.

Navigation
Data management → Security → OPC UA security



Certificate	Designation	Extension	Upload/download via button
CA root certificate or certificate of the OPC-UA client [1]	Trusted issuer certificate	.der	Trusted issuer certificate
OPC-UA server private key (PEM) [2]	Device private key	.pem	Device private key
OPC-UA server certificate (DER) [1]	Signed public key	.der	Upload signed public key
			Download signed public key
Certificate revocation list (CRL) [1], if using a CA root certificate	Certificate revocation list	.crl	Upload certificate revocation list

1) Certificate format as per: https://tools.ietf.org/html/rfc2585.
2) Certificate format as per: https://tools.ietf.org/html/rfc1421.

Maximum size of RSA key: 1024 bits. The size of the generated private key may not exceed 1024 bits.

If the OPC-UA server private key (device private key) matches the OPC-UA server certificate (signed public key), these are marked as available.

The OPC-UA server certificate (signed public key) can be uploaded at any time via "Upload signed public key".

If the IP address or the tag name is changed, the security certificates used must also be changed accordingly!

5.2.4 Changing the WLAN mode of the device to WLAN client

- The WLAN mode only needs to be changed if the device is integrated via WLAN!
- By activating the **WLAN Client** option, the device mode changes from an access point to a client. This action terminates any WLAN connection that is already established, e.g. to configure the parameters via the integrated Web server!

▶ **WLAN mode** parameter: select **WLAN Client** option.
↳ The device mode changes from an access point to a client.

Navigation
"Expert" menu → Communication → WLAN settings → WLAN mode

Parameter overview with brief description

Parameter	Description	Selection	Factory setting
WLAN mode	Select WLAN mode.	▪ WLAN access point ▪ WLAN Client	WLAN access point

5.3 Establishing a connection between the OPC-UA client and the device

Only one OPC-UA client can access the device at any one time.

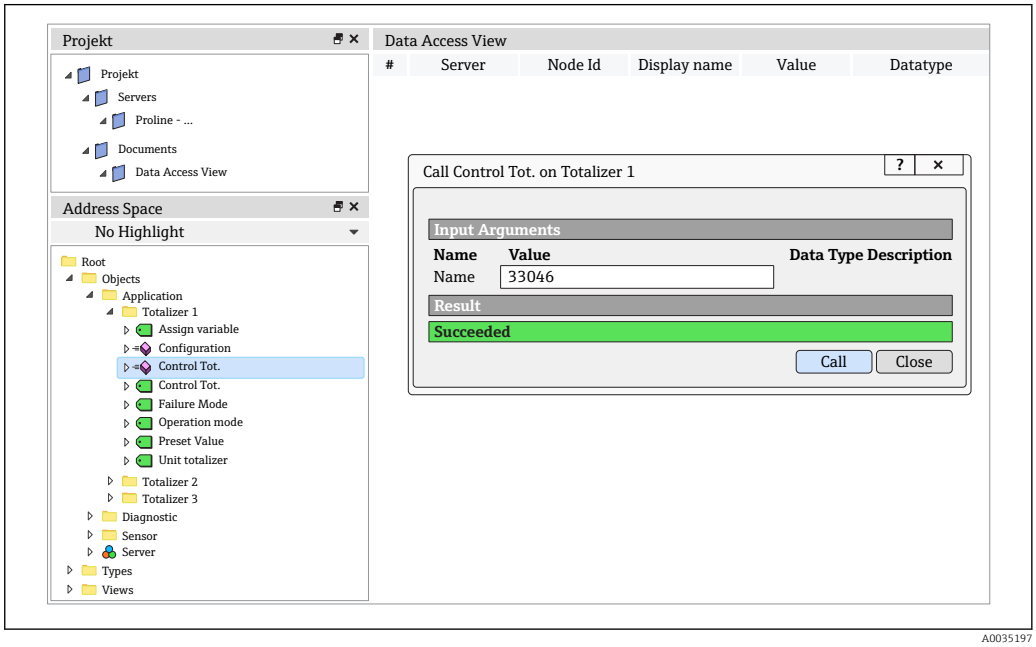
1. Starting the OPC-UA client
2. Search for the device via the URI (urn:dev:mac:<MAC address of the Ethernet interface>), e.g. urn:dev:mac:00070511131d
3. Select the device using the SSID name, e.g. EH_Promass_300_A802000
4. Enter the password for the device: in the case of devices supplied with the package ex-works, enter the serial number (Ser. No) e.g. L100A802000 indicated on the nameplate → 1, 4
   ↳ The OPC-UA client is connected to the OPC-UA server of the device and can access the device.

- If the IP address or the tag name is changed, the security certificates used must also be changed accordingly!
- For information on the device-specific security, user name and password, see → 10.

6 Operation

6.1 Information model

The parameters are saved in a specific structure. Users navigate through folders to get to the individual parameters.



3 *Example: visualization of the OPC-UA server in an OPC-UA client*

Navigation	Parameter	#	Type of information
Sensor → Meas. variables → Process variab. →	Mass flow	1	AnalogItemType
Sensor → Meas. variables → Process variab. →	Volume flow	2	AnalogItemType
Sensor → Meas. variables → Process variab. →	Corr.Vol.-flow	3	AnalogItemType
Sensor → Meas. variables → Process variab. →	Density	4	AnalogItemType
Sensor → Meas. variables → Process variab. →	Ref. density	5	AnalogItemType
Sensor → Meas. variables → Process variab. →	Temperature	6	AnalogItemType
Sensor → Meas. variables → Process variab. →	Pressure value	7	AnalogItemType
Sensor → Meas. variables → Process variab. →	Dynam. viscosity	8	AnalogItemType
Sensor → Meas. variables → Process variab. →	Kinematic visc.	9	AnalogItemType
Sensor → Meas. variables → Process variab. →	TempCompDynVisc.	10	AnalogItemType
Sensor → Meas. variables → Process variab. →	TempCompKinVisc.	11	AnalogItemType
Sensor → Meas. variables → Process variab. →	Concentration	12	AnalogItemType
Sensor → Meas. variables → Process variab. →	Target mass flow	13	AnalogItemType
Sensor → Meas. variables → Process variab. →	Carrier mass flow	14	AnalogItemType
Sensor → Meas. variables → Totalizer →	Totalizer val.1	15	AnalogItemType
Sensor → Meas. variables → Totalizer →	Totalizer val.2	16	AnalogItemType
Sensor → Meas. variables → Totalizer →	Totalizer val.3	17	AnalogItemType
Sensor → Meas. variables → Totalizer →	Tot. overflow 1	18	float_t
Sensor → Meas. variables → Totalizer →	Tot. overflow 2	19	float_t

Navigation	Parameter	#	Type of information
Sensor → Meas. variables → Totalizer →	Tot. overflow 3	20	float_t
Sensor → Meas. variables → Output Values →	Output curr. 1	21	AnalogItemType
Sensor → Meas. variables → Output Values →	Measur. Curr. 1	22	AnalogItemType
Sensor → System units →	Mass flow unit	23	MultiStateDiscreteType
Sensor → System units →	Mass unit	24	MultiStateDiscreteType
Sensor → System units →	Volume flow unit	25	MultiStateDiscreteType
Sensor → System units →	Volume unit	26	MultiStateDiscreteType
Sensor → System units →	Corr. vol. flow unit	27	MultiStateDiscreteType
Sensor → System units →	Corr. vol. flow unit	28	MultiStateDiscreteType
Sensor → System units →	Density unit	29	MultiStateDiscreteType
Sensor → System units →	Ref. dens. unit	30	MultiStateDiscreteType
Sensor → System units →	Temperature unit	31	MultiStateDiscreteType
Sensor → System units →	Pressure unit	32	MultiStateDiscreteType
Sensor → System units →Date→	Time format	33	MultiStateDiscreteType
Application → Totalizer 1 →	Assign variable	34	MultiStateDiscreteType
Application → Totalizer 1 →	Unit totalizer	35	MultiStateDiscreteType
Application → Totalizer 1 →	Operation mode	36	MultiStateDiscreteType
Application → Totalizer 1 →	Control Tot.	37	MultiStateDiscreteType
Application → Totalizer 1 →	Preset value	38	float_t
Application → Totalizer 1 →	Failure mode	39	MultiStateDiscreteType
Application → Totalizer 2 →	Assign variable	40	MultiStateDiscreteType
Application → Totalizer 2 →	Unit totalizer	41	MultiStateDiscreteType
Application → Totalizer 2 →	Operation mode	42	MultiStateDiscreteType
Application → Totalizer 2 →	Control Tot.	43	MultiStateDiscreteType
Application → Totalizer 2 →	Preset value	44	float_t
Application → Totalizer 2 →	Failure mode	45	MultiStateDiscreteType
Application → Totalizer 3 →	Assign variable	46	MultiStateDiscreteType
Application → Totalizer 3 →	Unit totalizer	47	MultiStateDiscreteType
Application → Totalizer 3 →	Operation mode	48	MultiStateDiscreteType
Application → Totalizer 3 →	Control Tot.	49	MultiStateDiscreteType
Application → Totalizer 3 →	Preset value	50	float_t
Application → Totalizer 3 →	Failure mode	51	MultiStateDiscreteType
Sensor → Testpoints →	Osc. freq. 0	52	AnalogItemType
Sensor → Testpoints →	Signal asymmetry	53	AnalogItemType
Sensor → Testpoints →	Exc. current 0	54	AnalogItemType
Sensor → Testpoints →	Osc. damping 0	55	AnalogItemType
Sensor → Testpoints →	HBSI	56	AnalogItemType
Sensor → Testpoints →	Carr. pipe temp.	57	AnalogItemType
Sensor → Testpoints →	Osc. freq. 1	58	AnalogItemType
Sensor → Testpoints →	Freq. fluct. 0	59	AnalogItemType
Sensor → Testpoints →	Freq. fluct. 1	60	AnalogItemType
Sensor → Testpoints →	Osc. ampl. 0	61	AnalogItemType
Sensor → Testpoints →	Osc. ampl. 1	62	AnalogItemType

Navigation	Parameter	#	Type of information
Sensor → Testpoints →	Osc. damping 1	63	AnalogItemType
Sensor → Testpoints →	Exc. current 1	64	AnalogItemType
Diagnostics → Heartbeat →	Verific. report	65	File_t
Diagnostics → Heartbeat →	Plant operator	66	String
Diagnostics → Heartbeat →	Location	67	String
Diagnostics →	Actual diagnos.	68	String

6.2 Application example

6.2.1 Configuring the totalizer

1. In the OPC-UA client navigate to the parameters for totalizer 1: Application → Totalizer 1
2. Parameter Control Tot. – Enter input arguments for totalizer control and confirm with Call

Configuration of the Control Tot. parameter

Input arguments	Possible options
Control totalizer	▪ 32226 (0): Add ▪ 32490 (1): Reset and stop ▪ 32228 (2): Default value and stop ▪ 198 (3): Reset and add ▪ 199 (4): Default value and add ▪ 32928 (3): Stop

3. Parameter configuration – enter input arguments for the various configurations and confirm with Call.

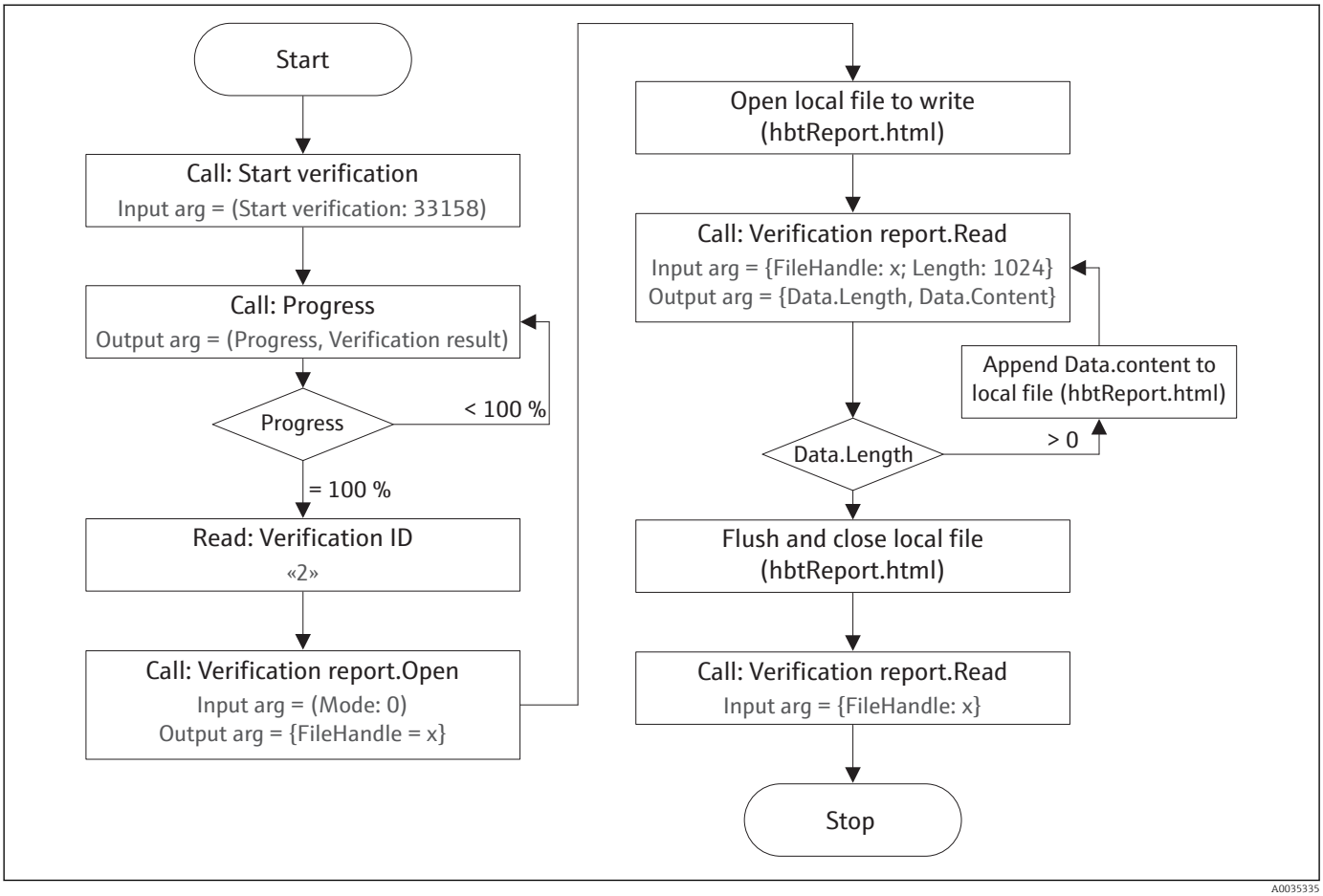
Configuration of the Configuration parameter

Input arguments	Possible options
Assign process variable	▪ 32961 (0): Mass flow ▪ 33122 (1): Volume flow ▪ 33093 (2): Corrected volume flow ▪ 901 (13): Target mass flow ▪ 793 (14): Carrier mass flow ▪ 900 (39): Target volume flow ▪ 3097 (40): Carrier volume flow ▪ 3094 (37): Target corrected volume flow ▪ 3096 (38): Carrier corrected volume flow ▪ 3041 (42): GSV flow ▪ 3042 (43): Alternative GSV flow ▪ 3044 (44): NSV flow ▪ 3043 (45): Alternative NSV flow ▪ 3045 (46): S&W volume flow ▪ 3051 (52): Oil mass flow ▪ 3054 (55): Water mass flow ▪ 3049 (50): Oil volume flow ▪ 3052 (53): Water volume flow ▪ 3050 (51): Oil corrected volume flow ▪ 3053 (54): Water corrected volume flow
Totalizer operation mode	▪ 33306 (0): Net total flow ▪ 33028 (1): Forward flow total ▪ 32976 (2): Reverse flow total
Failure mode	▪ 276 (0): Stop ▪ 33061 (1): Current value ▪ 32970 (2): Last valid value

Input arguments	Possible options		
Preset value	Floating point number with sign		
Unit totalizer	Mass unit ▪ 1089 (60): g ▪ 1088 (61): kg ▪ 1092 (62): t ▪ 1093 (125): oz ▪ 1094 (63): lb ▪ 1095 (64): STon ▪ 1997 (251): None	Volume unit ▪ 1571 (240): cm^3 ▪ 1035 (240): dm^3 ▪ 1034 (43): m^3 ▪ 1040 (240): ml ▪ 1038 (41): l ▪ 1041 (236): hl ▪ 32805 (240): Ml Mega ▪ 1572 (240): af ▪ 1043 (112): ft^3 ▪ 1570 (240): fl oz (us) ▪ 1048 (40): gal (us) ▪ 1648 (240): kgal (us) ▪ 32806 (240): Mgal (us) ▪ 1051 (46): bbl (us;oil) ▪ 1052 (152): bbl (us;liq.) ▪ 1641 (170): bbl (us;beer) ▪ 32808 (240): bbl (us;tank) ▪ 1049 (42): gal (imp) ▪ 32807 (42): Mgal (imp) ▪ 32810 (240): bbl (imp;beer) ▪ 32809 (240): bbl (imp;oil)	Corrected volume unit ▪ 1574 (167): NL ▪ 1573 (166): Nm^3 ▪ 1575 (240): Sm^3 ▪ 1053 (168): Sft^3 ▪ 32852 (240): Sgal (us) ▪ 32857 (240): Sbbl (us;liq.) ▪ 32862 (240): Sgal (imp)

6.3 Heartbeat Verification

6.3.1 Heartbeat Verification flowchart



4 *Performing Heartbeat Verification, opening and saving the verification report*

6.3.2 Performing Heartbeat Verification

1. In the OPC-UA client navigate to the parameters for Heartbeat: Diagnostic → Heartbeat
2. Parameter Start verificat. – Input arguments: enter 33158 (start) and confirm with Call
3. Parameter Progress – Output Arguments: the progress of the verification and the current verification results are displayed.
   ↳ When the verification progress bar reaches 100%, the result 33245 (Done) is displayed.

Possible display values for Verific. results – Output Arguments:
- 33242 (0): Busy
- 33245 (0): Done
- 33161 (0): Not done
- 275 (2): Failed

4. Call up the result of a verification via Verification Results – Input Arguments: enter the verification number and confirm with Call.
   ↳ The result of the selected verification is displayed (see the following table).

Only the last eight verifications can be called.

Call Verific. results on Heartbeat

Output arguments	Possible results
Date/Time	Time of verification
Overall result	▪ 890 (0): Passed ▪ 32996 (250): Not passed ▪ 33161 (0): Not done ▪ 2280 (0): Not plugged ▪ 275 (2): Failed
Sensor	
HBSI	
Sensor electronic module (ISEM)	
I/O Module	
System status	

7 Technical data

7.1 OPC-UA certification

The device complies with the "Nano Embedded Server Profile" defined in OPC-UA Standard Part 7 – Release 1.03, §6.5.53.

7.2 OPC-UA methods

The devices supports the following OPC-UA methods:
- Application/Totalizer x/Configuration (in:process variable, in:unit totalizer, in:operation mode, in:preset value, in:failure mode) (x=1, 2, 3)
- Application/Totalizer x/Control Tot. (in: control tot.) (x=1, 2, 3)
- Diagnostics/Heartbeat/timestamp (in: year, in: month, in: day, in: hour, in: minute)
- Diagnostics/Heartbeat/start verification (in: start verification)
- Diagnostics/Heartbeat/Progress (out: Progress, out: Verific. results)
- Diagnostics/Heartbeat/Verification Results (in: Verification ID, out: date/time, out: overall result, out: sensor, out: HBSI, out: Sens. electronic, out: I/O module, out: system status)

7.3 OPC-UA clients

All OPC-UA clients that are certified in compliance with OPC-UA can be connected to the OPC-UA server of the device.

Transport layer	The connection can only be via the OPC-UA TCP transport protocol in accordance with the OPC-UA Standard Specification, Document OPC UA, Part 6, Release 1.03.
Data encryption	The OPC-UA client can only communicate with the device via OPC-UA binary encryption. For information on OPC-UA binary encryption: see the OPC-UA Standard Specification, Document OPC UA Part 6, Release 1.03

7.4 Technical requirements

Computer: configure OPC-UA parameters	For the configuration of the OPC UA parameters of the device. Connect the computer via the service interface (CDI-RJ45) of the device. **Hardware** - Interface: the computer must have an RJ45 interface. - Connection: standard Ethernet cable with RJ45 connector. - Screen: recommended size: ≥ 12" (depends on the screen resolution). **Software** Recommended operating systems: Microsoft Windows 7 or higher. **User rights** User rights (e.g. administrator rights) are required for TCP/IP and proxy server settings.

Computer: integrate the device into a plant network	For the integration of the device into a plant network. **Software: supported OPC-UA clients** All commercially available OPC-UA clients and toolkits, such as: ▪ "UA Expert" from Unified Automation ▪ Prosys OPC UA Client from Prosys OPC ▪ PI System from OSIsoft ▪ Various SCADA packages with an OPC-UA interface **Network connections** A network connection to the plant network is required.
Mobile operating unit (e.g. smart phone, tablet): integrate the device into a plant network	For integrating the device into a plant network. **Hardware** ▪ Interface: the mobile operating unit (e.g. smart phone, tablet) must have a WLAN interface. ▪ Connection: connection established via WLAN. **Software: supported OPC-UA clients** All commercially available OPC-UA clients and toolkits, such as: ▪ Prosys OPC UA Client from Prosys OPC ▪ Various SCADA packages with an OPC-UA interface **Network connections** A network connection to the plant network is required.

8 Appendix

8.1 OPC-UA parameters

8.1.1 "OPC-UA configuration" submenu

Navigation Expert → Communication → OPC-UA configuration

▶ **OPC-UA configuration**		
	Activate OPC-UA function	→ 30
	Application URI	→ 30
	UTC date and time	→ 31
	▶ **OPC-UA settings**	→ 31
	▶ **OPC-UA security**	→ 36

Activate OPC-UA function

Navigation Expert → Communication → OPC-UA configuration → Activate OPC-UA function

Description Activate the OPC-UA function.

Selection
- No
- Yes

Factory setting No

Application URI

Navigation Expert → Communication → OPC-UA configuration → Application URI

Description Displays the name of the OPC-UA application.

User interface Character string

Factory setting urn:dev:mac:(MAC Adrdress)

UTC date and time

Navigation Expert → Communication → OPC-UA configuration → UTC date and time

Description Displays the date and time used by the OPC-UA server.

The device displays 1.1.1970 the first time it is powered up. The device adopts the time and date from the OPC-UA client once it is integrated.

User interface Character string

Factory setting 1.1.1970

"OPC-UA settings" submenu

Navigation Expert → Communication → OPC-UA configuration → OPC-UA settings

▶ OPC-UA settings	
Application name	→ 31
Port	→ 32
Minimum publishing interval	→ 32
Minimum sampling interval	→ 32
▶ OPC-UA date and time	→ 33

Application name

Navigation Expert → Communication → OPC-UA configuration → OPC-UA settings → Application name

Description Displays the name which is used to identify the OPC-UA server.

User interface Corresponds to the name of the measuring point in the **Device tag** parameter.

Factory setting Promass

Port

Navigation Expert → Communication → OPC-UA configuration → OPC-UA settings → Port

Description Define the TCP/IP port which is to be used to establish the connection to the OPC-UA server.

Note the following when defining the TCP/IP port:
- Recommendation: keep the standard TCP/IP port.
- Do not use the same TCP/IP port that is already being used for the Web server.
- Define a TCP/IP port > 49152.

User entry Positive integer

Factory setting 4840

Minimum publishing interval

Navigation Expert → Communication → OPC-UA configuration → OPC-UA settings → Minimum publishing interval

Description Displays the minimum publishing time for the values for cyclic data exchange.

User interface Positive integer [ms]

Factory setting 1000 ms

Minimum sampling interval

Navigation Expert → Communication → OPC-UA configuration → OPC-UA settings → Minimum sampling interval

Description Displays the minimum sampling interval for the values for cyclic data exchange.

The OPC-UA client may not access the values for cyclic data exchange faster than the minimum sampling interval indicated here.

User interface Positive integer [ms]

Factory setting 1000 ms

"OPC-UA date and time" submenu

Navigation Expert → Communication → OPC-UA configuration → OPC-UA settings → OPC-UA date and time

▶ OPC-UA date and time	
UTC date and time	→ 31
Year	→ 33
Month	→ 34
Day	→ 34
Hour	→ 34
Minute	→ 35
Set system time	→ 35

UTC date and time

Navigation Expert → Communication → OPC-UA configuration → OPC-UA settings → OPC-UA date and time → UTC date and time

Description Displays the date and time used by the OPC-UA server.

The device displays 1.1.1970 the first time it is powered up. The device adopts the time and date from the OPC-UA client once it is integrated.

User interface Character string

Factory setting 1.1.1970

Year

Navigation Expert → Communication → OPC-UA configuration → OPC-UA settings → OPC-UA date and time → Year

Prerequisite The **Yes** option is selected in the **Set system time** parameter (→ 35) parameter.

Description Select the year for the system time set manually.

User entry 9 to 99

Factory setting 10

Month

Navigation Expert → Communication → OPC-UA configuration → OPC-UA settings → OPC-UA date and time → Month

Prerequisite The **Yes** option is selected in the **Set system time** parameter (→ 35) parameter.

Description Select the month for the system time set manually.

Selection
- January
- February
- March
- April
- May
- June
- July
- August
- September
- October
- November
- December

Factory setting January

Day

Navigation Expert → Communication → OPC-UA configuration → OPC-UA settings → OPC-UA date and time → Day

Prerequisite The **Yes** option is selected in the **Set system time** parameter (→ 35) parameter.

Description Select the day for the system time set manually.

User entry 1 to 31 d

Factory setting 1 d

Hour

Navigation Expert → Communication → OPC-UA configuration → OPC-UA settings → OPC-UA date and time → Hour

Prerequisite The **Yes** option is selected in the **Set system time** parameter (→ 35) parameter.

Description Select the hour for the system time set manually.

User entry 0 to 23 h

Factory setting 12 h

Minute

Navigation Expert → Communication → OPC-UA configuration → OPC-UA settings → OPC-UA date and time → Minute

Prerequisite The **Yes** option is selected in the **Set system time** parameter (→ 35) parameter.

Description Enter the minute for the system time set manually.

User entry 0 to 59 min

Factory setting 0 min

Set system time

Navigation Expert → Communication → OPC-UA configuration → OPC-UA settings → OPC-UA date and time → Set system time

Prerequisite The **Yes** option is selected in the **Set system time** parameter (→ 35) parameter.

Description Choose between the system time from the OPC-UA client or the system time set manually.

- System time from OPC-UA client: **No** option
- System time set manually: **Yes** option

Selection
- No
- Yes

Factory setting No

"OPC-UA security" submenu

The security setting and the required certificates for a connection to the OPC-UA server of the device are defined in the **OPC-UA security** submenu (→ 36).

Navigation Expert → Communication → OPC-UA configuration → OPC-UA security

▶ OPC-UA security	
Security policy	→ 36
Available security files	→ 36

Security policy

Navigation Expert → Communication → OPC-UA configuration → OPC-UA security → Security policy

Description Select the security policy.

Selection
- None
- Signed Basic128Rsa15
- Signed and encrypted Basic128Rsa15

Factory setting None

Available security files

Navigation Expert → Communication → OPC-UA configuration → OPC-UA security → Available security files

Description List of the available security certificates and certificate revocation list.

User interface
- Trusted issuer certificate
- Device private key
- Signed public key
- Certificate revocation list

www.addresses.endress.com

Endress+Hauser

People for Process Automation