

JUMO flowTRANS MAG H20

JUMO DELOS S02



Security Manual



40505600T95Z001K000

V1.00/EN/2026-01-12

Further information and downloads



qr-405056-en.jumo.info



qr-406065-en.jumo.info

Table of contents

1	About this documentation	4
1.1	Validity	4
1.2	Applicable documentation	4
1.3	Purpose	4
1.4	Target group	4
1.5	Definition of terms	5
1.6	Symbols	5
2	Safety	6
2.1	Intended use	6
2.2	Qualification of personnel	6
3	Interfaces	7
3.1	Local interfaces	7
3.2	Network interfaces (Ethernet)	8
3.2.1	Security Consideration	8
4	Organizational measures of the operator	10
4.1	Data management	10
4.2	Software update	10
4.3	Measures for device security settings	10
4.3.1	Authentication	10
5	Organizational measures of the manufacturer	12
5.1	Development process	12
5.2	Dealing with security gaps	12

1 About this documentation

1.1 Validity

Device	Device version
JUMO DELOS S02	SPE
JUMO DELOS S02	IO-Link
JUMO flowTRANS MAG H20	SPE
JUMO flowTRANS MAG H20	IO-Link

1.2 Applicable documentation

Product group	Document name	Document type
405056	JUMO DELOS S02 – Pressure transmitter with display, device version with SPE	Operating Manual 40505612T90Z001K000
405056	JUMO DELOS S02 – Pressure transmitter with display, device version with IO-Link	Operating Manual 40505611T90Z001K000
406065	JUMO flowTRANS MAG H20 – Electromagnetic flowmeter for liquids, device version with SPE	Operating Manual 40606512T90Z001K000
406065	JUMO flowTRANS MAG H20 – Electromagnetic flowmeter for liquids, device version with IO-Link	Operating Manual 40606511T90Z002K000

1.3 Purpose

The document contains the assessment and guidelines for product security of the listed devices.

The document is intended to convey knowledge, provide assistance when making decisions and promote measures in the field of Security.

1.4 Target group

This documentation is intended to be used by personnel for plant mechanical systems for sanitary, heating and air-conditioning technology, electrical engineering or mechanical and plant engineering throughout all phases of the product life cycle.

1.5 Definition of terms

Use in the documentation	Definition
Device, product	Pressure transmitter, flowmeter
Product lifecycle	Overall consideration of Product identification, acceptance of the goods, storage, mounting, connection, operation, troubleshooting, maintenance to disposal
User	Operator, system integrator
End device	Smartphone, tablet, laptop, PC etc.
Trusted zone	Area within a network or system with a high level of security and protection
JUMO smartCONNCET App	Software for configuration and parameterization
Cloud Gateway	Component for secure connection to cloud services and resources
JUMO Cloud	IoT platform for process visualization, data acquisition, data analysis and data archiving
Security-by-Design	Strategy for integrating security measures into the architecture and design during the planning and development phase of the device
Secure Implementation	Practical execution and compliance with the security requirements defined in Security-by-Design through secure and error-free implementation

1.6 Symbols



NOTE!

This symbol is used in tables and indicates that further information is provided after the table.



REFERENCE!

This symbol refers to **further information** in other sections, chapters, or other manuals.

2 Safety

2.1 Intended use

Use the devices exclusively in accordance with the intended use specified in the respective operating manual.

⇒ chapter 1.2 "Applicable documentation", Page 4.

2.2 Qualification of personnel

The personnel deployed must meet the following requirements for all work steps on the system:

- Have completed their technical training and are qualified
- Have been authorized by the operator
- Are familiar with the Security Manual

The functional requirements of the local and network-based interfaces ensure the necessary IT security environment.

To define the IT security environment, the application areas that the manufacturer has based its security considerations on are presented.

3.1 Local interfaces

The device was designed for installations within a restricted-access facility. In this context, the trust boundary in the device's security assessment was defined by the enclosure, and therefore unauthorized opening of the device was not considered.

IO-Link	
Function	Bidirectional transmission of process values, diagnostic data, configuration data, and device information within a trusted zone, display of process values The impact of a failure must be considered by the operator/system integrator.
Communication	Via end device with IO-Link master and device description file (IODD)
Authentication	–
Wireless 	
Function	Bidirectional transmission of process values and configuration data
Communication	Via end device with JUMO smartCONNECT app
Authentication	Via Bluetooth (BLE 5.1) and NFC tag

Wireless

The focus was on the security objective of data integrity. Measures to maintain confidentiality were not implemented.

The interface is not designed for continuous operation with regard to availability. It is intended exclusively for device configuration during commissioning and for device testing as part of diagnostics.

For secure authentication of the smartConnect app to the device, an NFC-based pairing procedure is used. Authentication is performed via a near-field challenge-response method that ensures the unique identity of the app.

This procedure guarantees that pairing can only be carried out on-site by the user.

The integrity of data transmission between the smartConnect app and the device is protected against bit errors using CRC32.

⇒ chapter 4.3.1 "Authentication", Page 10.

Prevent unauthorized access by non-authorized persons or machines through organizational measures (e.g., access controls, device monitoring, locking the control cabinet).

3 Interfaces

3.2 Network interfaces (Ethernet)

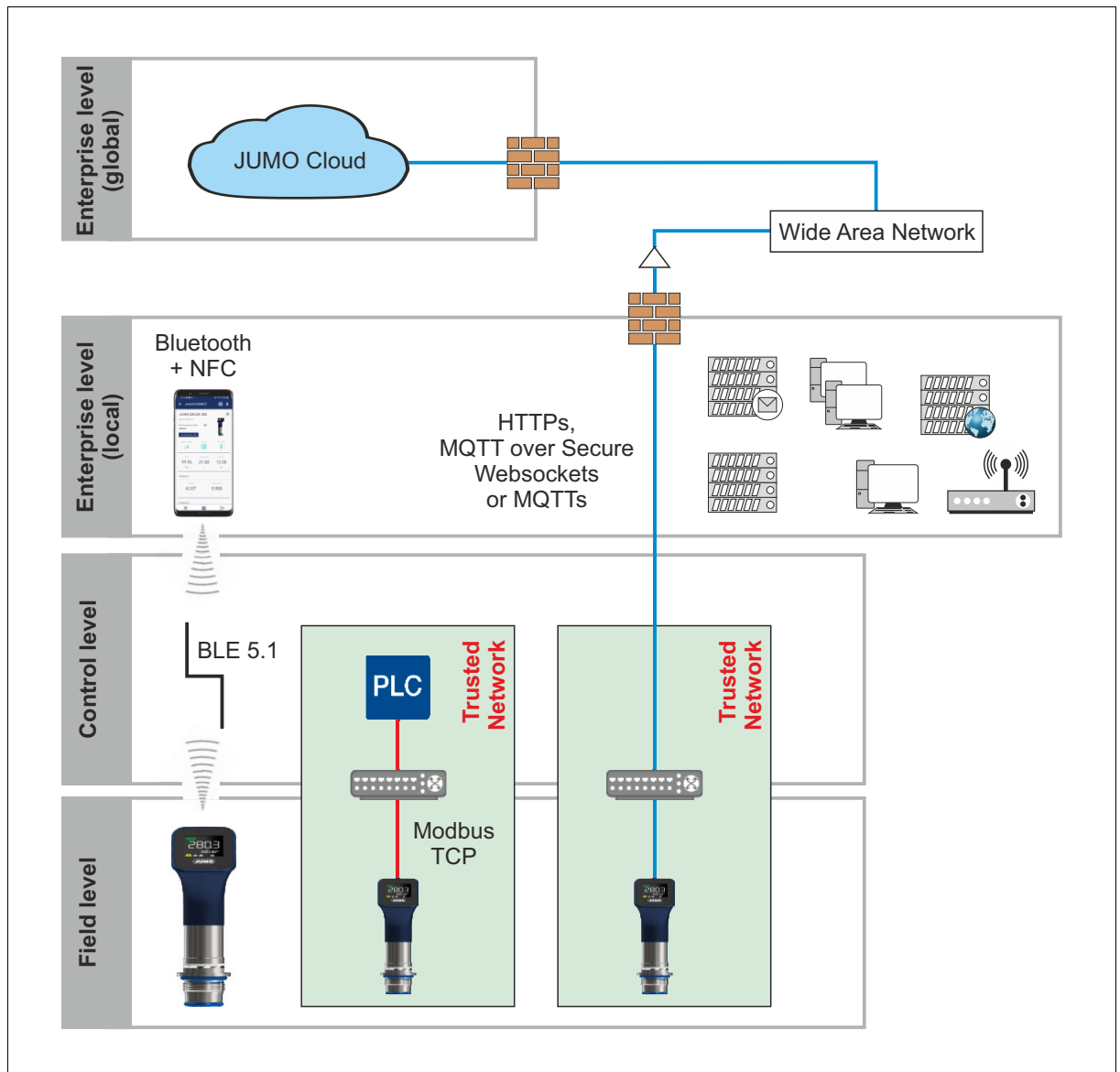
The safety considerations apply to device versions with SPE.

3.2.1 Security Consideration

The architecture illustrates a typical application of the device with a network interface at the field level. The system architecture into which the device is integrated may include the following elements:

- Device
- JUMO smartCONNECT app
- JUMO Cloud

The figure shows that the device must be integrated into a trusted network zone. For the safety considerations, two independent use cases can be distinguished, which can be integrated individually or in combination into the desired system.



System Monitoring via Cloud Gateway (Red Line)

Function	Transmission of process values and status information
Communication	Via Cloud Gateway to JUMO Cloud, unidirectional through Cloud Gateway with data diode
Authentication	User ID and password
Protocol	
HTTPs client	Communication to JUMO Cloud (Port 443)
MQTTs	Communication to JUMO Cloud via WebSocket Secure or MQTTs (Port 443)
Display	
Cloud Gateway connection	JUMO Cloud
Device error	Symbol on device display

The port specifications refer to the default settings of the Cloud Gateway. If the parameter "Cloud Server" is set to "Custom," the data connection is switched to a different port and the data protocol is changed. In this case, the port number is defined:

Port specifications	Protocol
wss://<host>:<port>/<path> Example: wss://xyz.net:443	MQTT via WebSocket Secure (default: Port 443) MQTT via WebSocket Secure via port 443
https://<host>:<port>/<path> Example: mqttts://xyz.net:1883	MQTTs (default: Port 443) MQTTs via Port 1883

Measurement data acquisition and system configuration via Modbus TCP (Blue Line)

The device optionally features an SPE interface.

Function	Transmission of process data, configuration data, and device information Usage must be evaluated by the operator/system integrator.
Communication	Via Modbus TCP slave
Authentication 	—

Authentication

Modbus TCP communication is not protected by technical measures by the manufacturer and is therefore not suitable for use in a non-trusted network. Securing the Modbus TCP interface must be carried out as part of a risk assessment by the system integrator.

4 Organizational measures of the operator

4.1 Data management

For proper use, the device does not need any personal data, traffic data or location data and does not have any corresponding protective measures.

The transfer of money, monetary assets, or virtual currencies is not admissible.

Personal data, financial data, or billing data which can be traced back to individuals are not part of the manufacturer's security appraisal.

When dealing with personal data according to GDPR (General Data Protection Regulation; in German: DSGVO), as per (EU 2016/679), suitable data protection measures are required.

4.2 Software update

The device does not have an automatic software update (e.g., OTA update).

- The operator secures the software update via the IO-Link interface.
- Do not switch off the device during the software update.
- Repeat the software update in case of a power failure.
- After a software update via the smartConnect App, observe the organizational measures.

The current software is available via email: support@jumo.net

4.3 Measures for device security settings

The document does not claim to be an exhaustive record of security measures.

The system integrator or operator conducts a complete security check of the system.

The measures to reduce security-critical aspects of the system apply to startup and ongoing operation of the device.

The measures include the settings on the device via the configuration parameters and ensure protection against unauthorized access.

4.3.1 Authentication

Bluetooth

When connecting in an untrusted environment, observe the following:

- After commissioning the device, set the parameter "Bluetooth Mode" to the value "Restricted". Changing the parameter ensures that after the initial NFC pairing, no permanent connection exists between the device and the mobile terminal.
- Repeat authentication via NFC pairing whenever the mobile terminal loses connection to the device, e.g., due to range limitations.
- Deactivate the Bluetooth interface using the parameter "Bluetooth Mode". Reactivation is only possible via the IO-Link or Modbus TCP interface.

4 Organizational measures of the operator

Cloud-Gateway

Unauthorized access can lead to data loss and data manipulation, which may impair operation and data security.

To ensure device security, observe the following:

- Change the passwords of preconfigured users during commissioning.
- Change passwords if there are signs of unauthorized access.
- Assign each user only the rights that are absolutely necessary for performing their tasks (principle of least privilege).
- Guidance for creating secure passwords:
 - ⇒ Federal Office for Information Security (BSI): [Sichere Passwörter erstellen](#).

5 Organizational measures of the manufacturer

5.1 Development process

The development process is governed by DIN EN ISO 9001 and is audited cyclically by independent bodies.

The IEC 62443-4-1 specifies the requirements for a secure product lifecycle for hardware and software components. Cybersecurity aspects are directly integrated into the product development process, ensuring device security from the very beginning of development.

The further development takes cybersecurity aspects into account according to the following principles:

- Security by Design
- Secure Implementation

5.2 Dealing with security gaps

During the device development process, organizational measures base on IEC 62443-4-1 minimize product security risks caused by vulnerabilities when the device placed on the market by the manufacturer.

A Product Security Incident Response process provided by JUMO ensures during the device's series production phase that reported vulnerabilities are addressed and communicated.

For information on reported vulnerabilities and on how to report them, refer to the JUMO website:

<https://www.jumo.group/de/en/services/product-security>



JUMO GmbH & Co. KG

Street address:
Moritz-Juchheim-Straße 1
36039 Fulda, Germany

Delivery address:
Mackenrodtstraße 14
36039 Fulda, Germany

Postal address:
36035 Fulda, Germany

Phone: +49 661 6003-0
Fax: +49 661 6003-607
Email: mail@jumo.net
Internet: www.jumo.net

JUMO UK LTD

JUMO House
Temple Bank, Riverway
Harlow, Essex, CM20 2DY, UK

Phone: +44 1279 63 55 33
Fax: +44 1279 62 50 29
Email: sales@jumo.co.uk
Internet: www.jumo.co.uk

JUMO Process Control, Inc.

6724 Joy Road
East Syracuse, NY 13057, USA

Phone: +1 315 437 5866
Fax: +1 315 437 5860
Email: info.us@jumo.net
Internet: www.jumousa.com

