JUMO variTRON 300
JUMO variTRON 500 touch

Security Manual

70500000T95Z001K000

V1.00/EN/2025-02-18

Further information and downloads

qr-705002-en.jumo.info

qr-705003-en.jumo.info

qr-705004-en.jumo.info

Table of contents

1 About this documentation

1.1 Validity

The documentation is valid for the software versions of the following devices:

Device	From software version
JUMO variTRON 300	431.8.2.0
JUMO variTRON 500 touch	446.8.4.0

1.2 Applicable documentation

Product group	Document name	Document type
705002	JUMO variTRON – automation system	System overview 70500200T10Z100K000
705003	JUMO variTRON 300 – automation system – central processing unit	Operating manual 70500300T90Z000K000
705004	JUMO variTRON 500 touch – automation system – central processing unit	Operating manual 70500400T90Z000K000

1.3 Purpose

The document includes the evaluation and Security guidelines of the JUMO variTRON 300 and JUMO variTRON 500 touch.

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 trained electrical, automation technology, mechanical, and plant engineering personnel across all phases of the product lifecycle. Qualified personnel with PLC programming skills are required for the necessary interventions within the CODESYS development environment.

1.5 Definition of terms

Use in the documentation	Definition
Device, product	Automation system – central processing unit
Product lifecycle	Overall consideration of Product identification, acceptance of the goods, storage, mounting, connection, operation, troubleshooting, maintenance to disposal

1.6 Symbols

NOTICE!

The signal word "NOTICE" indicates possible damage to property.

Non-observance can lead to damage to devices, systems or the environment.

▶ Observe the instructions in the note for avoiding damage!

REFERENCE!

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

2 Safety

2.1 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 plant operator
- Are familiar with the Security Manual and the security information and warnings contained within it

2.2 Unauthorized access

NOTICE!

Security gaps due to unauthorized access.

Unauthorized access may result in data loss and data manipulation, which has a negative impact on operation and data security.

▶ Secure access with technical and organizational measures (e.g. access controls, device monitoring, locking of the control cabinet), ⇨ page 7.

▶ Only assign each user the rights that are absolutely required to perform their work (principle of least privilege, ⇨ page 10).

3 Interfaces

This chapter describes the functional requirements of the local and network-based interfaces and the requirements to be implemented by the operator during system design by the system integrator in order to realize the IT security environment required by the manufacturer.

In order to define the IT security environment, the operator's areas of application which the manufacturer used as the basis for their security considerations are laid out in this chapter.

3.1 Local interfaces

The variTRON 300 (DIN-rail mounting) and the interfaces of the variTRON 500 touch (panel mounting) are intended for use within a control cabinet.
Observe the security information for unauthorized access, ⇨ page 6.

3.1.1 USB Host

The interface is intended for transmitting device data.

The mass storage device driver establishes the connection to USB interfaces such as memory sticks or hard disk drives. Access is managed via the device display and must be evaluated by the system integrator or operator with regard to security.
⇨ chapter 4.3.1 "User administration", Page 10

The interface is not hardened within the operating system.

3.1.2 RS485

The interface is exclusively intended for data transmission within a "trusted zone". The manufacturer has not taken any technical security measures.

The interface is not intended for use in security-critical applications.

The operator or system integrator takes the impact of a potential interface failure into consideration.

3.1.3 Wireless

The variTRON 300 (optionally from system version 5) and the variTRON 500 touch (optionally from system version 8) have a wireless interface for transmitting measured values in a proprietary format.

The measuring probe (transmitter) communicates unidirectionally with the device (receiver) at an adjustable transmission interval. Communication is free of reaction due to the unidirectional connection.

Transmitter	JUMO Wtrans p	Product group 402060
	JUMO Wtrans B	Product group 707060
	JUMO Wtrans E01	Product group 902928, from system version 3
	JUMO Wtrans T	Product group 902930
Radio frequencies	Europe	868.4 MHz
	America, Australia, Canada, New Zealand	912.6 to 917.4 MHz

No security measures, such as anti-jamming or protection against sniffing, have been taken by the manufacturer for receiving measurement data.

The interface is not intended for use in security-critical applications.

3.1.4 UART Debug

The interface can only be accessed externally through the housing via a defined connector. The interface is enabled for reading and is available for write access with a password (security-by-default).
⇨ chapter 4.3 "Measures for device security settings", Page 10

3 Interfaces

3.2 Network interfaces (Ethernet)

3.2.1 Architecture

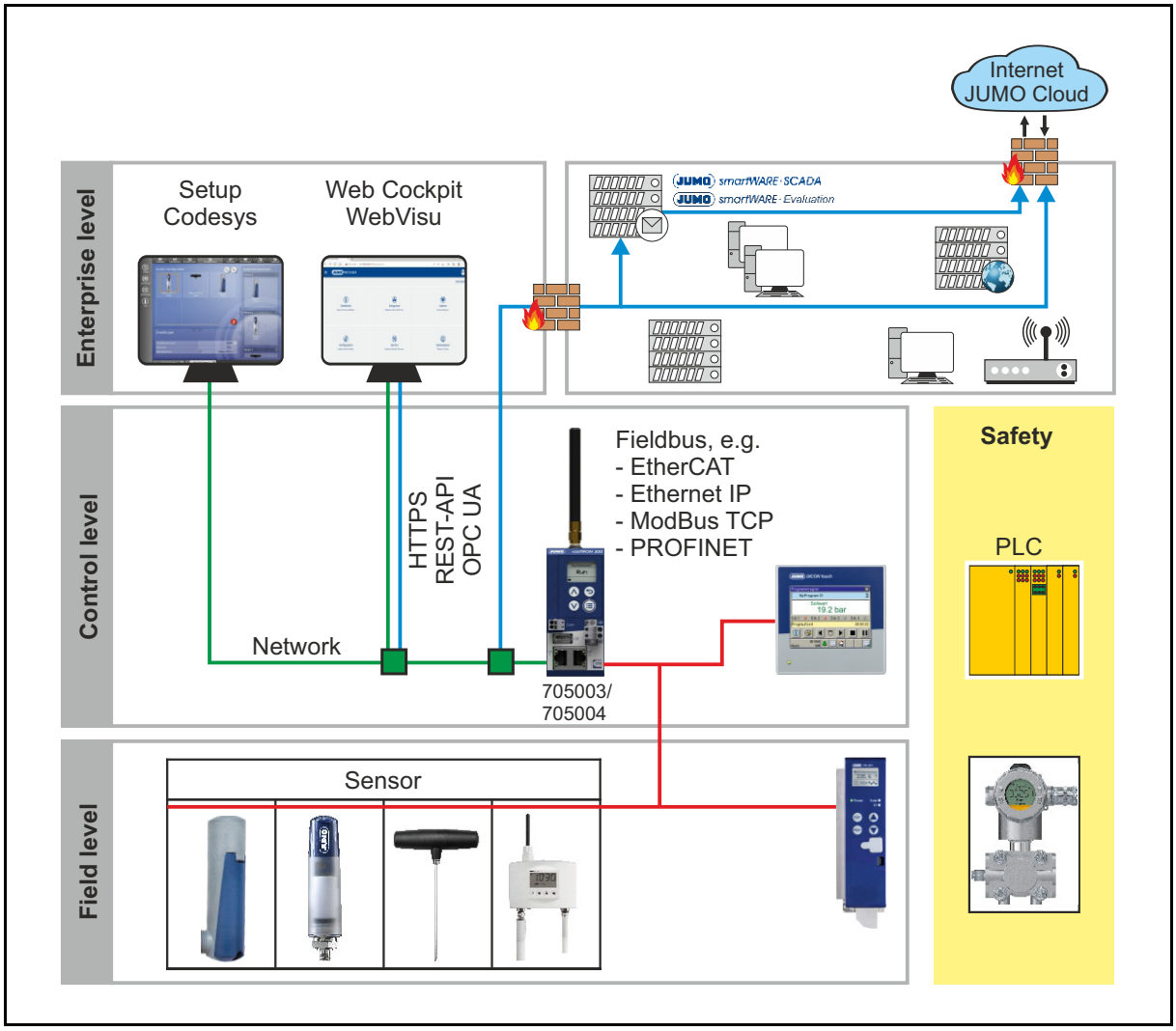

Fig. 3-1 Typical application of the device at the field or control level

The device system can consist of the following elements:

Designation	Description
705003/705004	Device
JUMO smartWARE Setup	Device configuration software (offline/online)
CODESYS	Development environment for PLC
Web Cockpit	Web applications for device configuration (online), online service tool
CODESYS WebVisu	Web application for displaying the masks created in CODESYS
JUMO smartWARE SCADA	Software for evaluating and visualizing process data and operation via web browser
JUMO Cloud	IoT platform for process visualization, data acquisition, data evaluation, and data archiving enables access to measurement data and operation via web browser
JUMO smartWARE Evaluation	Software for evaluating and visualizing process data via web browser

Implementation of the device in a trusted zone

Requirements:

- The operator or system integrator has protected the zone which the device is in against access from outside the zone, e.g. with a firewall.
- Setup PC software and CODESYS are installed on an end device (Windows Server® or Windows desktop PC).
- The operator or system administrator ensures the security of the end device and data archiving system (smartWARE Evaluation).
- Recommendation: The PC software is separated from the IT network by means of network segmentation (between local and public).

Criticality of communication channels

The chapter describes the Ethernet communication flows of data within the architecture.

Blue line

The channel transmits process data and historical data from the device to web applications, (JUMO Web Cockpit, CODESYS WebVisu, JUMO smartWARE SCADA, JUMO Cloud) and to the data archive system (Datastore of JUMO smartWARE Evaluation).

The data transmission between the device and the smartWARE Evaluation, WebCockpit or CODESYS WebVisu is realized by HTTP(s) communication. A HTTPs and MQTTs connection is used for communication with JUMO Cloud.

Data transmission is active during the entire lifecycle of the system.

Green line

The channel transmits configuration and user management data to set up the device.

Data transmission is time-limited and takes place locally in the plant during the system integration phase.

Data transmission is activated by means of a user request from the system integrator, who carries out the required data check for correctness.

Red line

The channel transmits data between the device and a local subordinate sensor or actuator (e.g. via Modbus TCP or JUMO system bus [JUMO controller modules, input modules, output modules]) or communicates between the device and a superordinate PLC (e.g. via PROFINET).

The fieldbus protocols do not support any security measures. A local network in the same segment within a trusted network can be established.

The system integrator should use a managed switch in order to disconnect the local sensor/actuator or PLC communication and the connection to the company level ("green line", "blue line") in various segments.

3.2.2 HTTP communication

External access to the system's HTTP communication is secured by means of cryptographic user verification with regard to authentication and authorization.

If incorrect user details are provided, the system returns the "401" HTTP response.

4 Organizational measures of the operator

4.1 Data storage

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 the Federal Data Protection Act, suitable data protection measures are required.

4.2 Firmwareupdate

The device does not support an automatic firmware update. The firmware update is performed by the operator or system integrator themselves.

The firmware update is available to download on the website.

NOTICE!

Data loss and impact on operation and data security due to unauthorized access.

▶ Assign the "Firmware update" right to a trustworthy person,
⇨ Operating manual, chapter "User rights".

4.3 Measures for device security settings

NOTICE!

Security gaps in the system.

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

▶ A complete security check of the system must be performed by the system integrator or the operator.

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 User administration

NOTICE!

Security gaps due to unauthorized access.

Unauthorized access may result in data loss and data manipulation, which has a negative impact on operation and data security.

▶ Guide for assigning secure passwords:
⇨ German Federal Office for Information Security (BSI): Creating Secure Passwords.

▶ Change passwords as soon as there are signs of unauthorized access.

▶ Only assign each user the rights that are absolutely required to perform their work (principle of least privilege).

To ensure device security, preconfigured user passwords must always be changed during startup.

The device does not have any mechanism for checking password rules. It is the operator's or system integrator's responsibility to adhere to password rules.

Device lockout is prevented if at least one user has the "UserManagement" right (⇨ Operating manual, chapter "User administration"). The user can grant or withdraw rights for themselves and other persons and must be considered separately within the operator's or system integrator's security appraisal.

4.3.2 Internal web server

The device has an internal web server that communicates with the application software (JUMO smartWARE Setup) and the device remote operation (Web Cockpit) via a RestAPI.

Communication takes place via the HTTP or HTTPs application protocols.

The configuration parameter "HTTP" is set to "inactive" for security communication (port 8090). Encrypted communication takes place exclusively via HTTPs via the port 8443.
⇨ Operating manual 705003, chapter "Web server"

4.3.3 Debug interface

The manufacturer protects write access to the debug interface against unauthorized access with a password.

The operator or system administrator can update the password to the debug interface to optimize security.

Procedure:

1. In the "Service" device menu, select the "Activate debug interface" function under "Device manager" (system version 6 and higher).
   By selecting the function, an automatic password is generated and stored in the event list.
2. Restart the device to deactivate the SSH interface.

5 Manufacturer measures

5.1 Development process

The development process includes design guidelines for designing software systems and quality assurance measures tailored to these.

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

The further development comprises cyber security with regard to security-by-design and secure implementation.

5.2 Dealing with security gaps

The device development process ensures reported security gaps are dealt with.

The service process maps reporting of security gaps during device distribution and considers analysis of and dealing with security gaps.

Security gaps are reported by email to Technical Support.

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