JUMO variTRON 300
JUMO variTRON 500 touch

Security Manual

70500000T95Z001K000

V2.00/EN/2025-12-03

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

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 70500200T10Z101K000
705003	JUMO variTRON 300 – Automation system – Central processing unit	Operating manual 70500300T90Z001K000
705004	JUMO variTRON 500 touch – Automation system – central processing unit	Operating manual 70500400T90Z001K000

1.3 Purpose

The document includes the evaluation and guidelines for product security 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 Trademark information

All trademarks and trade and company names used are the property of their rightful owners or authors.

1.6 Definition of terms

Use in the documentation	Definition
User	Operator, system integrator
CODESYS	Development environment for programming control systems (PLC)
Device, product	Automation system – central processing unit
IT security environment	Technical, organizational and legal framework conditions that influence the security of IT systems and data
JUMO Cloud	IoT platform for process visualization, data acquisition, data analysis and data archiving
JUMO smartWARE Evaluation	Software for evaluating and visualizing process data via web browser including datastore (data archving system)
JUMO smartWARE SCADA	Software for evaluation and visualization of process data and operation via web browser
JUMO smartWARE Setup	Device configuration software
JUMO-Systembus	Controller modules, input/output modules
End device	Smartphone, tablet, laptop, PC etc.
Managed Switch	Device for configuration, monitoring and controlling the network
Mass storage device driver	Software for controlling mass storage devices
Principle of Least Privilege	Security concept for defining the necessary access rights for users, programs or processes
Product lifecycle	Overall consideration of Product identification, acceptance of the goods, storage, mounting, connection, operation, troubleshooting, maintenance to disposal
SSH (Secure Shell)	Network protocol that establishes encrypted connections between computers for secure remote access
Trusted zone	Area within a network or system with a high level of security and protection
Web Cockpit	Web application for device configuration, online service tool
WebVisu	Web application for displaying the masks created in CODESYS

1.7 Symbols

⇨ **REFERENCE!**

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

2 Safety

2.1 Intended use

JUMO variTRON 300

The device is an automation platform.

The device serves a central control unit for small to medium-sized applications.

The device is used for managing configuration and parameter data and optionally provides a PLC.

JUMO variTRON 500 touch

The device is an automation platform with a touch control panel.

The device is used for controlling and visualizing industrial processes.

The devices are used in Industry 4.0 and IoT applications, e.g., within a control cabinet.

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

2.3 Unauthorized access

Unauthorized access can lead to data loss and data manipulation, endangering operations and data security.

- Secure access through technical and organizational measures (e.g. access controls, device monitoring, locking of the control cabinet), ⇨ page 7.
- Assign user rights according to the activity (Principle of Least Privilege, ⇨ page 10).

3 Interfaces

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

When using local interfaces, observe the safety information regarding unauthorized access.

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 user with regard to security, ⇨ page 10.

The interface is not protected within the operating system against external access or misuse.

3.1.2 RS485

The interface is used exclusively for data transmission within a "trusted zone".

The manufacturer has not implemented taken any technical security measures.

The user is responsible for considering the impact of a possible interface failure.

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.

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. The write access is protected by a password (security-by-default), ⇨ page 10.

3.2 Network interfaces (Ethernet)

3.2.1 Architecture

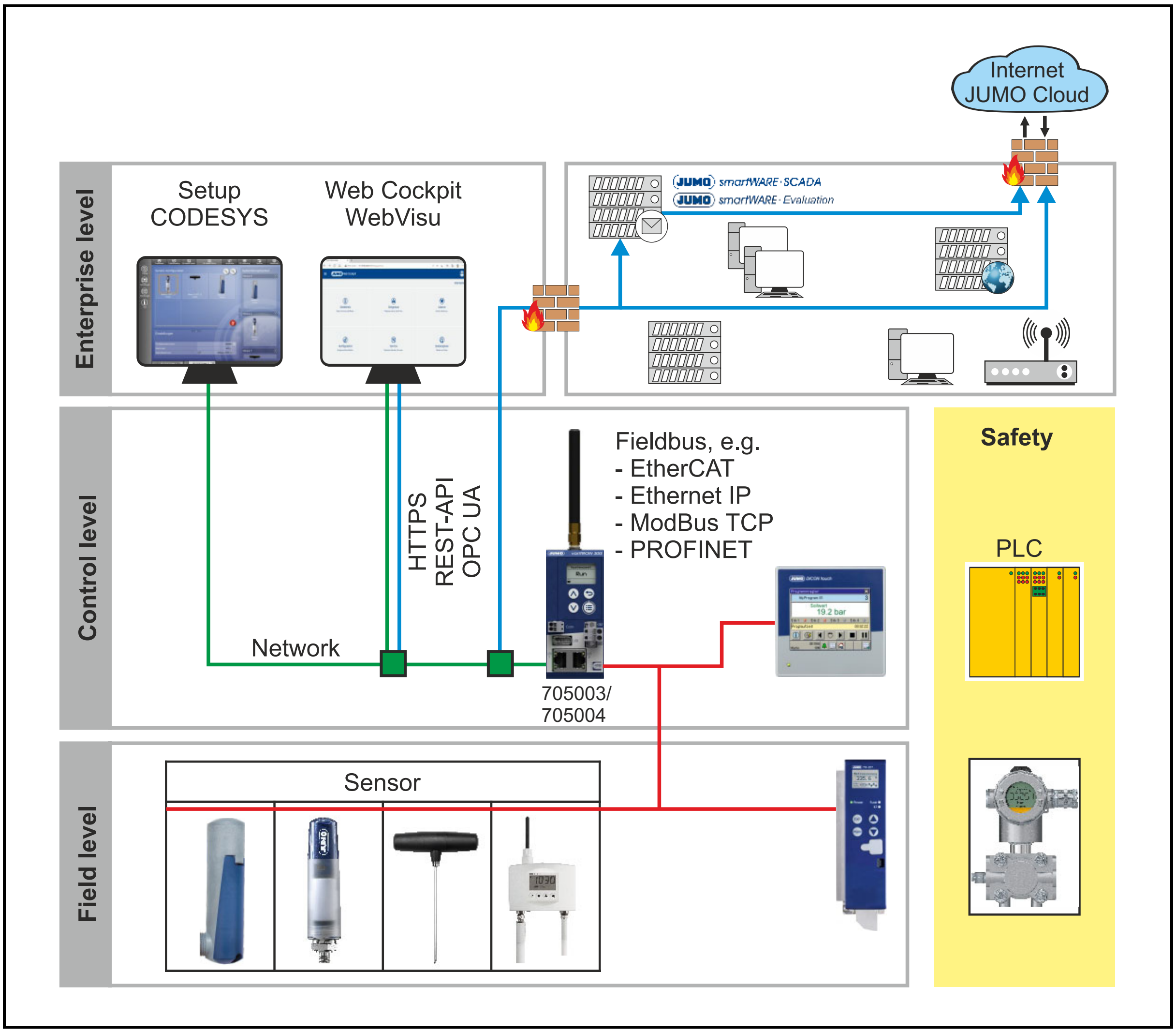

Fig. 3-1 Application example of the device at the field or control level

Typical system elements:

- Device
- JUMO smartWARE Setup
- CODESYS
- Web Cockpit
- WebVisu
- JUMO smartWARE SCADA
- JUMO Cloud
- JUMO smartWARE Evaluation

Implementation of the device in a trusted zone

Requirements:

- The user 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 user ensures the security of the end device and data archiving system.

Recommendation: The PC software is separated from the IT network by means of network segmentation (between local and public).

Criticality of communication channels

Within the architecture, a distinction is made between three data flows of Ethernet communication:

Blue line

The channel transmits process data and historical data from the device to web applications, and to the data archive system.

The data transmission is realized by HTTP(s) communication. The communication with the JUMO Cloud takes place via HTTPs and MQTTs connection.

Data transmission is active during the entire system lifecycle.

Green line

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

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

The data transmission is activated by means of a user request. The User 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) or communicates between the device and a superordinate PLC (e.g. via PROFINET).

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

The managed switch divides the field level (local sensor/actuator or PLC communication) and the enterprise level ("green line", "blue line") into different, separate network 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 the user information is incorrect, the system returns the HTTP response "401".

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 the Federal Data Protection Act (BDSG), BGBl. I S. 2097, suitable data protection measures are required.

4.2 Firmwareupdate

The firmware update is performed by the user themselves and is available to download on the website of the manufacturer.

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

4.3 Measures for device security settings

Security gaps in the system

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 User administration

The device security during startup is ensured by changing the passwords of preconfigured users.

It is the users responsibility to adhere to password rules.

Procedure:

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

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

2. Only assign each user the rights that are absolutely required to perform their work (Principle of Least Privilege).

Device lockout is prevented if at least one user has the right "UserManagement", ⇨ Operating manuals 705003 and 705004, chapter "User management".

The user can grant or withdraw rights for themselves and other persons and must be considered separately within the security appraisal.

4.3.2 Internal web server

The device has an internal web server that communicates with the setup software and Web Cockpit via the RestAPI interface.

Communication takes place via the HTTP or HTTPs protocols.

Validity	Example	Port
Version 8	446.8.X.X	8443
Version 9	446.9.X.X	443

The HttpMode is preset to "Redirect to HTTPS".
Requests to the web server are redirected from HTTP (port 80) to HTTPS (port 443), ensuring that only secure connections are possible by default.

In CODESYS WebVisu, the "CODESYS WebVisu Compatibility Mode" can be enabled as legacy support. Port 8080 opens, and CODESYS WebVisu is accessible.

If the HttpMode is set to "Active", legacy port 8080 also opens.

By default, compatibility mode is **not** enabled.

⇨ Operating manual, chapter "Web server"

4.3.3 Debug interface

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

The user can update the password to optimize security.

Procedure:

1. In the menu ***Service*** > ***Device manager***, select ***Activate debug interface*** (requirement: system version 6 or higher).
   By selecting the function, an automatic password is generated and stored in the event list.
2. Restart the device.
3. Deactivate the SSH interface.

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.de/web/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