JUMO variTRON 300
JUMO variTRON 500 touch

Security Manual

70500000T95Z000K000

V2.00/DE/2025-12-03

Weitere Informationen und Downloads

qr-705002-de.jumo.info

qr-705003-de.jumo.info

qr-705004-de.jumo.info

Inhalt

1 Zu dieser Dokumentation

1.1 Gültigkeit

Gerät	Ab Software-Version
JUMO variTRON 300	431.8.2.0
JUMO variTRON 500 touch	446.8.4.0

1.2 Mitgeltende Dokumentation

Produktgruppe	Dokumentname	Dokumentart
705002	JUMO variTRON – Automatisierungssystem	Systemübersicht 70500200T10Z100K000
705003	JUMO variTRON 300 – Automatisierungssystem – Zentraleinheit	Betriebsanleitung 70500300T90Z000K000
705004	JUMO variTRON 500 touch – Automatisierungssystem – Zentraleinheit	Betriebsanleitung 70500400T90Z000K000

1.3 Zweck

Das Dokument enthält die Bewertung und die Richtlinien zur Produkt-Security des JUMO variTRON 300 und des JUMO variTRON 500 touch.

Das Dokument dient der Vermittlung von Wissen, der Unterstützung bei Entscheidungen und der Förderung von Maßnahmen im Bereich der Security.

1.4 Zielgruppe

Diese Dokumentation richtet sich in allen Phasen des Produktlebenszyklus an ausgebildetes Personal der Elektrotechnik, Automatisierungstechnik und des Maschinen- und Anlagenbaus. Für die nötigen Eingriffe innerhalb der Entwicklungsumgebung von CODESYS ist Fachpersonal mit SPS-Programmierkenntnissen erforderlich.

1.5 Markenrechtliche Hinweise

Alle verwendeten Marken sowie Handels- und Firmennamen sind Eigentum ihrer rechtmäßigen Eigentümer oder Urheber.

1.6 Begriffsdefinitionen

Verwendung in der Dokumentation	Definition
Benutzer	Betreiber, Systemintegrator
CODESYS	Entwicklungsumgebung für die Programmierung von Steuerungen (SPS)
Gerät, Produkt	Automatisierungssystem – Zentraleinheit
IT-Sicherheitsumfeld	Technische, organisatorische und rechtliche Rahmenbedingungen, die die Sicherheit von IT-Systemen und Daten beeinflussen
JUMO Cloud	IoT-Plattform zur Prozessvisualisierung, Datenerfassung, Datenauswertung und Datenarchivierung
JUMO smartWARE Evaluation	Software zur Auswertung und Visualisierung von Prozessdaten über Webbrowser inkl. Datastore (Datenarchivsystem)
JUMO smartWARE SCADA	Software zur Auswertung und Visualisierung von Prozessdaten und Bedienung über Webbrowser
JUMO smartWARE Setup	Software zur Gerätekonfiguration
JUMO-Systembus	Reglermodule, Ein-/Ausgangsmodule
Endgerät	Smartphone, Tablet, Laptop, PC etc.
Managed Switch	Gerät zur Konfiguration, Überwachung, Steuerung des Netzwerks
Mass-Storage-Device-Treiber	Software zur Steuerung von Massenspeichergeräten
Principle of Least Privilege	Sicherheitskonzept zur Festlegung der notwendigen Zugriffsrechte für Benutzer, Programme oder Prozesse
Produktlebenszyklus	Gesamtbetrachtung von Produktidentifizierung, Lagerung, Anschluss, Montage, Betrieb, Störungsbeseitigung, Wartung bis Entsorgung
SSH (Secure Shell)	Netzwerkprotokoll, das verschlüsselte Verbindungen zwischen Computern für einen sicheren Fernzugriff herstellt
Vertrauenswürdige Zone	Bereich innerhalb eines Netzwerks oder Systems mit einem hohen Maß an Sicherheit und Schutz
Web Cockpit	Webanwendung zur Gerätekonfiguration, Online-Servicetool
WebVisu	Webanwendung zur Darstellung der in CODESYS erstellten Masken

1.7 Symbole

VERWEIS!

Dieses Zeichen weist auf **weitere Informationen** in anderen Abschnitten, Kapiteln oder anderen Anleitungen hin.

2 Sicherheit

2.1 Bestimmungsgemäße Verwendung

JUMO variTRON 300

Das Gerät ist eine Automatisierungsplattform.

Das Gerät dient als zentrale Steuereinheit für kleine bis mittlere Anwendungen.

Das Gerät wird zur Verwaltung von Konfigurations- und Parameterdaten eingesetzt und stellt optional eine SPS zur Verfügung.

JUMO variTRON 500 touch

Das Gerät ist eine Automatisierungsplattform mit Touch-Bedienpanel.

Das Gerät eignet sich zur Steuerung und Visualisierung von industriellen Prozessen.

Die Geräte werden in Industrie 4.0- und IoT-Anwendungen eingesetzt, z. B. innerhalb eines Schaltschranks.

2.2 Qualifikation des Personals

Für alle Arbeitsschritte am System wird Personal mit folgenden Eigenschaften vorausgesetzt:

- Technisch ausgebildet und qualifiziert
- Autorisiert vom Betreiber
- Vertraut mit dem Security Manual

2.3 Unbefugte Zugriffe

Unbefugte Zugriffe können zu Datenverlust und Datenmanipulation führen. Betrieb und Datensicherheit sind gefährdet.

- Zugriffe durch technische und organisatorische Maßnahmen (z. B. Zugangskontrollen, Überwachung des Geräts, Abschließen des Schaltschranks) sichern, ⇨ Seite 7.
- Benutzerrechte der Tätigkeit entsprechend zuweisen (Principle of least privilege, ⇨ Seite 10).

Die funktionalen Anforderungen der lokalen und netzwerkbasierten Schnittstellen gewährleisten das notwendige IT-Sicherheitsumfeld.

Zur Definition des IT-Sicherheitsumfelds werden die Anwendungsbereiche dargestellt, die der Hersteller bei seinen Sicherheitsüberlegungen zugrunde gelegt hat.

3.1 Lokale Schnittstellen

Bei Verwendung der lokalen Schnittstellen den Sicherheitshinweis für unbefugte Zugriffe beachten.

3.1.1 USB-Host

Die Schnittstelle dient zur Übertragung von Gerätedaten.

Der Mass-Storage-Device-Treiber stellt die Verbindung zu USB-Schnittstellen, wie Speichersticks oder Festplatten, her. Der Zugriff wird über das Gerätedisplay gesteuert und muss vom Benutzer bezüglich der Security bewertet werden, ⇨ Seite 10.

Die Schnittstelle ist innerhalb des Betriebssystems nicht gegen Zugriffe von Außen oder Missbrauch geschützt.

3.1.2 RS485

Die Schnittstelle dient ausschließlich zur Datenübertragung innerhalb einer „vertrauenswürdigen Zone“.

Der Hersteller hat keine technischen Maßnahmen zur Security getroffen.

Der Benutzer berücksichtigt den Einfluss eines möglichen Ausfalls der Schnittstelle.

3.1.3 Funk

Der variTRON 300 (optional ab Systemversion 5) und der variTRON 500 touch (optional ab Systemversion 8) verfügen über eine Wireless-Schnittstelle zur Messwertübertragung im proprietären Format.

Der Messwertgeber (Sender) kommuniziert in einem einstellbaren Sendeintervall unidirektional mit dem Gerät (Empfänger). Die Kommunikation ist rückwirkungsfrei.

Sender	JUMO Wtrans p	Produktgruppe 402060
	JUMO Wtrans B	Produktgruppe 707060
	JUMO Wtrans E01	Produktgruppe 902928, ab Systemversion 3
	JUMO Wtrans T	Produktgruppe 902930
Funkfrequenzen	Europa	868,4 MHz
	Amerika, Australien, Kanada, Neuseeland	912,6 bis 917,4 MHz

Für den Messdatenempfang wurden keine Security-Maßnahmen, wie Anti-Jamming oder Schutz vor Sniffing, vom Hersteller getroffen.

Die Schnittstelle ist nicht für den Einsatz in security-kritischen Anwendungen geeignet.

3.1.4 UART Debug

Die Schnittstelle ist von außen nur über einen definierten Stecker durch das Gehäuse erreichbar. Die Schnittstelle ist zum Lesen freigeschaltet. Der Schreibzugriff ist über ein Passwort gesichert (Security-by-Default), ⇨ Seite 10.

3 Schnittstellen

3.2 Netzwerkschnittstellen (Ethernet)

3.2.1 Architektur

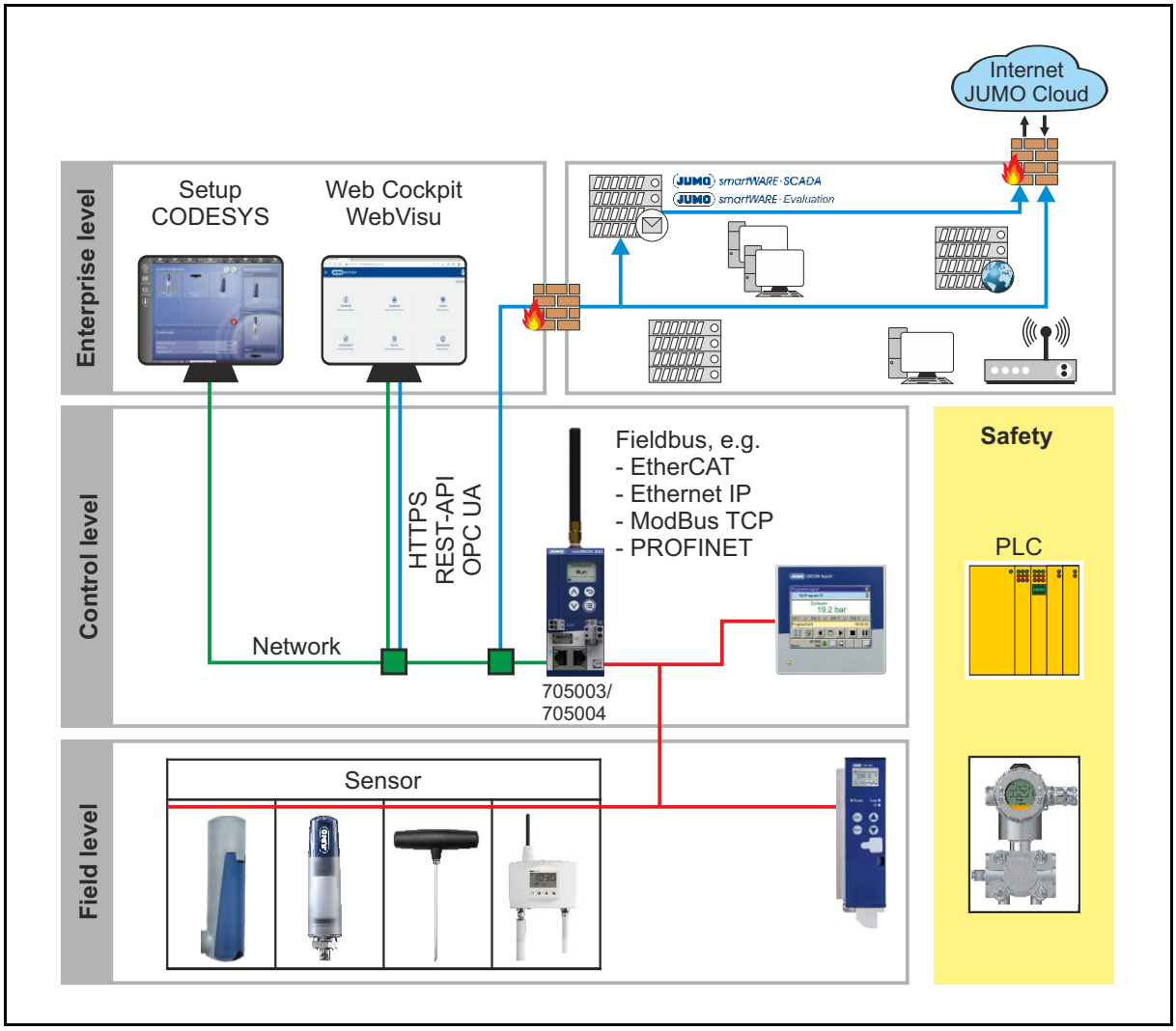

Abb. 3-1 Anwendungsbeispiel des Geräts auf der Feld- oder Leitebene

Typische Systemelemente:

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

Implementierung des Geräts in eine vertrauenswürdige Zone

Voraussetzungen:

- Der Benutzer hat die Zone, in der sich das Gerät befindet, vor Zugriffen von Außerhalb geschützt, z. B. durch eine Firewall.
- Die PC-Software Setup und CODESYS sind auf einem Endgerät (Windows-Server oder Windows-Desktop-PC) installiert.
- Der Benutzer gewährleistet die Sicherheit des Endgeräts und des Datenarchivierungssystems.

Empfehlung: Die PC-Software ist durch Netzwerksegmentierung (zwischen lokal und öffentlich) vom IT-Netzwerk getrennt.

Kritikalität der Kommunikationskanäle

Innerhalb der Architektur wird zwischen drei Datenflüssen der Ethernetkommunikation unterschieden:

Blaue Linie

Der Kanal überträgt Prozessdaten und historische Daten vom Gerät zu Webanwendungen sowie zum Datenarchivsystem.

Die Datenübertragung wird durch eine HTTP(s)-Kommunikation realisiert. Die Kommunikation zur JUMO Cloud erfolgt über eine HTTPs- und MQTTs-Verbindung.

Die Datenübertragung ist während des gesamten Systemlebenszyklus aktiv.

Grüne Linie

Der Kanal überträgt Konfigurations- und Benutzerverwaltungsdaten zur Einrichtung des Geräts.

Die Datenübertragung ist während der Systemintegrationsphase zeitlich begrenzt und erfolgt lokal im Werk.

Die Datenübertragung wird durch eine Benutzeranforderung aktiviert. Der Benutzer führt die erforderliche Datenprüfung durch.

Rote Linie

Der Kanal überträgt Daten zwischen dem Gerät und einem lokalen unterlagerten Sensor oder Aktor (z. B. über Modbus TCP oder JUMO-Systembus) bzw. kommuniziert zwischen dem Gerät und einer übergeordneten SPS (z. B. über Profinet).

Feldbus-Protokolle unterstützen keine Security-Maßnahmen. Ein lokales Netzwerk innerhalb eines bestimmten Bereiches kann im gleichen Segment betrieben werden, wenn dies als vertrauenswürdiges Netzwerk gilt.

Der Managed Switch teilt die Feldebene (lokale Sensor/Aktor- oder SPS-Kommunikation) und den Enterprise level (Grüne Linie, Blaue Linie) in verschiedene, voneinander abgetrennte Netzwerksegmente auf.

3.2.2 HTTP-Kommunikation

Der externe Zugriff auf die HTTP-Kommunikation des Systems ist durch einen kryptografischen Benutzernachweis in Bezug auf Authentifizierung und Authorisierung gesichert.

Bei falschen Benutzerangaben sendet das System die HTTP-Antwort „401“ zurück.

4 Organisatorische Maßnahmen des Betreibers

4.1 Datenverwaltung

Das Gerät benötigt für seine bestimmungsgemäße Verwendung keine personenbezogenen Daten, Verkehrsdaten oder Standortdaten und besitzt keine entsprechenden Schutzmaßnahmen.

Die Übertragung von Geld, monetären Werten oder virtuellen Währungen ist nicht zulässig.

Personenbezogene Daten, Finanzdaten oder Abrechnungsdaten, die Rückschlüsse auf Personen ermöglichen, sind nicht Teil der Sicherheitsbetrachtung durch den Hersteller.

Für den Umgang mit personenbezogenen Daten gemäß Bundesdatenschutzgesetz (BDSG), BGBl. I S. 2097, sind geeignete Maßnahmen zum Datenschutz erforderlich.

4.2 Firmwareupdate

Das Firmwareupdate wird vom Benutzer selbstständig durchgeführt und steht auf der Homepage des Herstellers zum Download zur Verfügung.

Das Recht „Firmwareupdate“ ausschließlich einer vertrauenswürdigen Person zuweisen, ⇨ Betriebsanleitung, Kapitel „Benutzerrechte“.

4.3 Maßnahmen für Security-Einstellungen des Geräts

Das Dokument erhebt keinen Anspruch auf Vollständigkeit der Security-Maßnahmen.

Der Systemintegrator bzw. Betreiber führt eine vollständige Sicherheitsüberprüfung des Systems durch.

Die Maßnahmen zur Reduzierung securitykritischer Aspekte der Anlage gelten für die Inbetriebnahme und den laufenden Betrieb des Geräts.

Die Maßnahmen umfassen die Einstellungen am Gerät über die Konfigurationsparameter und stellen einen Schutz vor unbefugten Zugriffen sicher.

4.3.1 Benutzerverwaltung

Die Gerätesicherheit bei der Inbetriebnahme wird durch Ändern der Passwörter vorkonfigurierter Benutzer gewährleistet.

Die Einhaltung der Passwortregeln liegt beim Benutzer.

Vorgehen:

1. Passwörter ändern, sobald Anzeichen für unbefugte Zugriffe bestehen.

   Orientierung zur Vergabe sicherer Passwörter:
   ⇨ Bundesamt für Sicherheit in der Informationstechnik (BSI): Sichere Passwörter erstellen.

2. Jedem Benutzer nur die Rechte zuordnen, die zur Ausführung seiner Tätigkeit unbedingt notwendig sind (Principle of least privilege).

Das „Aussperren“ vom Gerät wird verhindert, wenn mindestens ein Benutzer über das Recht „UserManagement“ verfügt, ⇨ Betriebsanleitungen 705003 und 705004, Kapitel „Benutzerverwaltung“.

Der Benutzer vergibt oder entzieht sich und anderen Rechte und ist innerhalb der Security-Betrachtung gesondert zu berücksichtigen.

4.3.2 Interner Webserver

Das Gerät verfügt über einen internen Webserver, der mit der Setup-Software und Web Cockpit über die Schnittstelle Rest API kommuniziert.

Die Kommunikation erfolgt über HTTP- bzw. HTTPS-Protokolle.

Gültigkeit	Beispiel	Port
Version 8	446.8.X.X	8443
Version 9	446.9.X.X	443

Der HttpMode ist auf „Umleitung auf HTTPS“ voreingestellt.
Anfragen an den Webserver werden über HTTP (Port 80) auf HTTPS (Port 443) umgeleitet, damit im Auslieferungszustand ausschließlich gesicherte Verbindungen möglich sind.

In der CODESYS WebVisu kann der „CODESYS WebVisu-Kompatibilitätsmodus“ als Legacy-Support aktiviert werden. Der Port 8080 öffnet sich und die CODESYS WebVisu ist erreichbar.

Wird der HttpMode auf „Aktiv“ gesetzt, öffnet sich der Legacy-Port 8080 ebenfalls.

Standardmäßig ist der Kompatibilitätsmodus **nicht** eingeschaltet.

⇨ Betriebsanleitung, Kapitel „Webserver“

4.3.3 Debug-Schnittstelle

Der Schreibzugriff gegen unbefugte Zugriffe ist vom Hersteller durch ein Passwort geschützt.

Der Benutzer kann zur Optimierung der Sicherheit das Passwort erneuern.

Vorgehen:

1. Im Gerätemenü ***Service*** > ***Gerätemanager*** die Funktion ***Debug-Schnittstelle aktivieren*** (Voraussetzung: Systemversion 6 oder höher) auswählen.
   Mit Auswahl der Funktion wird ein automatisches Passwort generiert und in die Ereignisliste gespeichert.
2. Das Gerät neu starten.
3. Die SSH-Schnittstelle deaktivieren.

5 Organisatorische Maßnahmen des Herstellers

5.1 Entwicklungsprozess

Der Entwicklungsprozess unterliegt der DIN EN ISO 9001 und wird zyklisch durch eine unabhängige Stelle auditiert.

Die IEC 62443-4-1 legt die Anforderungen an einen sicheren Produktlebenszyklus für Hard- und Softwarekomponenten fest. Cybersicherheitsaspekte werden unmittelbar in den Produktentwicklungsprozess integriert und gewährleisten die Sicherheit der Geräte von Beginn der Entwicklung an.

Die Weiterentwicklung berücksichtigt Cybersicherheitsaspekte nach folgenden Prinzipien:

- Security-by-Design
- Secure Implementation

5.2 Behandlung von Sicherheitslücken

Während des Entwicklungsprozesses des Geräts werden durch organisatorische Maßnahmen, angelehnt an die IEC 62443-4-1, die Risiken der Produktsecurity durch Sicherheitslücken beim Inverkehrbringen durch den Hersteller minimiert.

Ein durch JUMO bereitgestellter Product Security Incident Response-Prozess sorgt innerhalb der Serienphase des Geräts dafür, dass gemeldete Sicherheitslücken behandelt und für sie gemeldet werden.

Für Informationen zu gemeldeten Sicherheitslücken und zur Meldung von Sicherheitslücken die JUMO-Website beachten:

https://www.jumo.de/web/services/product-security

JUMO GmbH & Co. KG

Moritz-Juchheim-Straße 1
36039 Fulda, Germany

Telefon: +49 661 6003-727
Telefax: +49 661 6003-500
E-Mail: mail@jumo.net
Internet: www.jumo.net

Lieferadresse:
Mackenrodtstraße 14
36039 Fulda, Germany

Postadresse:
36035 Fulda, Germany

Technischer Support Deutschland:

Telefon: +49 661 6003-9135
Telefax: +49 661 6003-881899
E-Mail: support@jumo.net

JUMO Mess- und Regelgeräte GmbH

Pfarrgasse 48
1230 Wien, Austria

Telefon: +43 1 610610
Telefax: +43 1 6106140
E-Mail: info.at@jumo.net
Internet: www.jumo.at

Technischer Support Österreich:

Telefon: +43 1 610610
Telefax: +43 1 6106140
E-Mail: info.at@jumo.net

JUMO Schweiz AG

Laubisrütistrasse 70
8712 Stäfa, Switzerland

Telefon: +41 44 928 24 44
Telefax: +41 44 928 24 48
E-Mail: info.ch@jumo.net
Internet: www.jumo.ch

Technischer Support Schweiz:

Telefon: +41 44 928 24 44
Telefax: +41 44 928 24 48
E-Mail: info.ch@jumo.net