JUMO Cloud and JUMO smartWARE SCADA

Secure data management and FDA-compliant measured data recording





White paper

70181000T87Z001K000

V2.00/EN/30048756/2026-02-19

Table of contents

1 General information 4

1.1 Introduction 4
1.2 Implementation of Title 21 CFR Part 11 4
1.3 The system components of the IoT platform 4
1.4 The software components 5
1.4.1 Edge Gateway 5
1.4.2 JUMO Cloud 5
1.4.3 JUMO smartWARE SCADA 5

2 Requirement assessment 6

3 Reference list 16

1 General information

1.1 Introduction

In many areas of the manufacturing industry – especially in the pharmaceutical and food sectors – there is a mandatory requirement for product manufacturing documentation..

To record process and batch data, both paper-based chart recorders and paperless electronic screen recorders as well as PLC systems can be used. In order to securely store the recorded data over a long period and enable fast evaluation, stable and protected systems and IoT platforms are required.

The JUMO IoT platform for process visualization, data acquisition, analysis, and archiving allows worldwide – and, if necessary, locally restricted – access to measurement data via standard web browsers.

With JUMO Cloud, an online connection is required, enabling customers to securely access their data worldwide. If a customer prefers to manage their data and servers internally, JUMO smartWARE SCADA can be installed within the customer's network. Both solutions are designed on the same technical and visual basis.

For proper and clearly traceable recording of transmitted electronic process data, the U.S. **Food & Drug Administration (FDA)** issued 21 CFR Part 11 (Code of Federal Regulations) in 1997.

This regulation defines the requirements for **Electronic Records & Electronic Signatures**, meaning the paperless documentation of production processes as well as the electronic signature, which is equivalent to a handwritten signatur.

Compliance with the requirements of 21 CFR Part 11 forms the basis for worldwide acceptance of products in the pharmaceutical and food industries.

This "White Paper" provides the user with statements for each section of the legal text regarding how these requirements have been ensured.

1.2 Implementation of Title 21 CFR Part 11

JUMO meets the FDA requirements of 21 CFR Part 11 regarding "Electronic Records" and "Electronic Signature" with the software products and their functional properties specified in chapter 1.4 "The software components", Page 5.

1.3 The system components of the IoT platform

The IoT platform JUMO Cloud and JUMO smartWARE SCADA (hereinafter referred to as Cloud and SCADA) represent the following with their system components in accordance with 21 CFR Part 11:

- Open system for the Cloud
- Closed system for SCADA

1.4 The software components

1.4.1 Edge Gateway

The Edge Gateway is software that can be installed and operated on various hardware devices, PCs, or servers. It handles communication within the respective network and sends the collected information encrypted to the IoT platform. The Edge Gateway is implemented, among other things, in JUMO variTRON devices as well as in the intelligent JUMO sensors with Single Pair Ethernet (SPE) interface.

1.4.2 JUMO Cloud

The JUMO IoT platform for process visualization, data acquisition, analysis, and archiving enables worldwide access to measurement data via standard web browsers. With the JUMO Cloud, an Internet connection is required to allow customers to securely access their data worldwide.

1.4.3 JUMO smartWARE SCADA

If a customer wants to manage the IoT platform and their data themselves, JUMO smartWARE SCADA can be used and installed in the customer's network.
The JUMO IoT platform for process visualization, data acquisition, analysis, and archiving enables access to measurement data via standard web browsers and is designed visually and technically on the same basis as the JUMO Cloud.

2 Requirement assessment

The following explanations are based on the assumption that the reader is familiar with the basic requirements of 21 CFR Part 11.

Paragraph	Requirements: Subpart B: Electronic Records
§ 11.10	**Controls for closed systems**
Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:	
a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. **Requirement fulfilled!** • The system consists of the SCADA server and the associated edge gateways. Access to the system components is permitted only to authorized personnel. This access is protected against tampering by at least a username and password. • The control operation archive (audit trail) records all configuration and dashboard changes as well as data manipulations. Entries can be filtered. • Raw data (measurement data from edge gateways) cannot be modified at the application level. Setpoint changes or manual data entries within the application are logged and flagged in the control operation archive. • Secure and encrypted data transmission from the edge gateway to the server. **Responsibility of the System Owner:** Access to the hardware on which the edge gateway is installed, as well as to the SCADA server, must be protected against unauthorized access to prevent tampering.
b)	The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records. **Requirement fulfilled!** • All data can be exported in various formats either via export or directly from the database and made accessible to third parties. • With VPN access, it is possible to view process values directly through the user interface. Only a browser with a user account is required. • The reporting function allows individual reports to be generated and automatically provided to third parties as PDFs, for example via email.

Paragraph	Requirements: Subpart B: Electronic Records
§ 11.10	**Controls for closed systems**
c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.  • All data is stored in the SCADA server's database. • There is an option to set up high availability, where at least two servers operate redundantly. • The data stored on the SCADA server can be exported and archived by authorized personnel. • Access to the application is protected by username and password. Optionally, two-factor authentication and additional features (such as password policies) can be implemented via IAM (Identity Access Management). • The entire SCADA system (including all data) can be secured and restored through an automated or manual backup concept. **Responsibility of the System Owner:** Access protection and archiving of the stored data must be carried out by the system owner.
d)	Limiting system access to authorized individuals.  • At the beginning, rights are assigned and extended as needed by the SCADA system administrator stored in the IAM. • Access to the software components is restricted to authorized personnel through the assignment of different permissions. • Each user must log in with a username and password. Optionally, two-factor authentication and additional IAM functions can be used. • Changing user permissions may only be performed by authorized personnel. • Data that has already been stored and archived remains unchanged even when permissions are modified. **Responsibility of the System Owner:** System access must be defined, configured, and verified by the system owner..

2 Requirement assessment

Paragraph	Requirements: Subpart B: Electronic Records
§ 11.10	**Controls for closed systems**
e)	Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.  • The audit trail function is displayed via the so-called control operation archive. It records changes at the application level (dashboard and configuration) and on the gateways (send configuration). • The audit trail is generated automatically and cannot be configured or disabled within the application. • It is ensured that all relevant actions triggered by operating personnel are automatically recorded with date and time and stored in the audit trail. • Audit trail data cannot be modified or deleted within the application. • Audit trail data can be made accessible to all users at any time for review (dashboard).
f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.  • The sequence of steps, such as batch logging, is predefined. This allows configuration of whether an action should be executed for batch logging or not. • With a maintenance module, it is possible to create documentation for the execution of work instructions (Standard Operating Procedures “SOPs”).
g)	Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.  • At the beginning, rights are assigned and extended as needed by the SCADA system administrator stored in the IAM. • Access to the software components is restricted through the assignment of different permissions. • Access rights are checked and managed in the system by the IAM. • Only authorized personnel with the appropriate rights can create, block, or delete users. Historical activities of deleted users remain preserved even after deletion. • A prerequisite for a user’s system access is always login via a unique user ID (at least: username and password). • The use of a password can be time-limited by the administrator. After this period expires, the user must enter a new password or lose access authorization. Additional password policy settings are also possible within the scope of the IAM.

Paragraph	Requirements: Subpart B: Electronic Records
§ 11.10	**Controls for closed systems**
h)	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.  • The IoT platform can only be configured or operated by authorized personnel. • An edge gateway is automatically linked to a device identification number, allowing clear assignment. **Responsibility of the System Owner:** The system owner must ensure that every edge gateway used in the system has a unique identification (device ID, password).
i)	Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.  • All persons involved in the development of the IoT platform and the associated edge gateway software have been trained on the contents and requirements of 21 CFR Part 11.
j)	The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.  • The texts prompting the electronic signature can be freely formulated by the user. **It is the responsibility of the system owner.**
k)	Use of appropriate controls over systems documentation including: 1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. 2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation. **Not applicable!** **It is the responsibility of the system owner.**

2 Requirement assessment

Paragraph	Requirements: Subpart B: Electronic Records
§ 11.30	**Controls for open systems**
Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in § 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	
	Requirement fulfilled! • When operating as an open system (cloud), end-to-end cryptographic methods according to the current state of the art are used. These ensure trustworthiness and protection against tampering during data transmission from the edge gateway to the cloud server. • The IAM system used has been designed and configured to meet the requirements of an open system. • Access protection at the system administrator level (IT) is granted exclusively to authorized internal personnel. Regular cloud users have no access. • The fulfilled and listed requirements in § 11.10 also apply, where applicable, to the open system described here.

Paragraph	Requirements: Subpart B: Electronic Records
§ 11.50	**Signature manifestations**
a)	Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: 1) The printed name of the signer; 2) The date and time when the signature was executed; and 3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.  • All of the above information is part of the digital signature.
b)	The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).  • All information (a)(1), (a)(2), and (a)(3) of this paragraph is subject to the same controls as electronic documents (authenticity, integrity, and confidentiality). • All information (a)(1), (a)(2), and (a)(3) of this paragraph is human-readable and transparently accessible depending on the assigned permissions.

2 Requirement assessment

Paragraph	Requirements: Subpart B: Electronic Records
§ 11.70	**Signature/record linking**
	Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.  • An electronic signature is always linked to a batch. • The signature is always tied to the logged-in user. • Only authorized personnel (configurable by the system owner) can electronically sign batches. Copying or forging is not possible using standard methods. • An electronic signature (batch verification) can be reset by authorized users within the “Configuration” and must then be performed again. A reset is detected and recorded in the audit log. The previously performed verification will remain available and accessible.

Paragraph	Requirements: Subpart C: Electronic Signatures
§ 11.100	**General requirements**
a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.  • The electronic signature is always linked to the logged-in user. • Only authorized personnel (configurable by the system owner) can electronically sign batches. Copying the signature or reassigning it is not possible.
b)	Before an organization establishes, assigns, certifies, or otherwise sanctions an in individual's electronic signature, or any element of such electronic signature, the organization shall verify the identify of the individual. **Not applicable!** **It is the responsibility of the system owner.**
c)	Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures. **Not applicable!** **It is the responsibility of the system owner.**
c) 1)	The certification shall be signed with a traditional handwritten signature and submitted in electronic or paper form. Information on where to submit the certification can be found on FDA's web page on Letters of Non-Repudiation Agreement. **Not applicable!** **It is the responsibility of the system owner.**
c) 2)	Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature. **Not applicable!** **It is the responsibility of the system owner.**

2 Requirement assessment

Paragraph	Requirements: Subpart C: Electronic Signatures
§ 11.200	**Electronic signature components and controls**
a) 1)	Electronic signatures that are not based upon biometric shall: Employ at least two distinct identification components such as an identification code and password.  • The signature is always linked to the logged-in user. This user can log in with at least a username and password.
i)	When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be excecuted using all electronic signature components; subsequent signings shall be excecuted using at least one electronic signature component that is only excecutable by, and designed to be used only by, the individual.  • At the beginning, each user must log in with a username and password. • When performing an electronic signature, at least one of the components must be re-entered for verification. **The configuration of the verification process is the responsibility of the system owner.**
ii)	When an individual excecutes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be excecuted using all of the electronic signature components.  • For every interrupted session, the user must log in again with a username and password.
a) 2) 3)	Electronic signatures that are not based upon biometrics shall: 2) Be used only by their genuine owners; and 3) Be administered and executed to ensure that attempted use of an individual‘s electronic signature by anyone other than it‘s genuine owner requires collaboration of two or more individuals.  • Through the IAM system, additional measures can be implemented alongside username and password to secure system login (e.g., two-factor authentication). This ensures that only the logged-in person performs the electronic signature. • Furthermore, a re-verification must be carried out when executing the electronic signature.
b)	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners. **Not applicable!**

Paragraph	Requirements: Subpart C: Electronic Signatures
§ 11.300	**Controls for identification codes/passwords**
Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:	
a)	Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.  • This requirement can be configured in the IAM system. **It is the responsibility of the system owner.**
b)	Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).  • This requirement can be configured in the IAM system. **It is the responsibility of the system owner.**
c)	Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.  • This requirement can be configured in the IAM system. **It is the responsibility of the system owner.**
d)	Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.  • This requirement can be configured in the IAM system. **It is the responsibility of the system owner.**
e)	Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner **Not applicable!**

3 Reference list

[1] Mass & Peither
AG GMP Publishing
21 CFR 210/211 cGMP FOR FINISHED PHARMACEUTICALS
(Current Good Manufacturing Practice for Finished Pharmaceuticals)
including 21 CFR 11 Electronic Records/Electronic Signature
(Electronic Documents/Electronic Signature
with German translation and keyword index

[2] US Website „Code of Federal Regulations“
www.ecfr.gov
Title 21/Chapter I/Subchapter A/Part 11



