Creating a 21CFR 11 compliant application with Inductive Automation

Copyright

Table of Contents

Introduction

The United States Food and Drug Administration requires certain manufacturing industries to maintain strict records. Title 21 Code of Federal Regulations Part 11 (21CFR11) is a comprehensive legislation that provides criteria for using electronic records and signatures in the place of their handwritten equivalents. It addresses confidentiality, authentication, integrity, availability, and non-repudiation. 21CFR11 further specifies details about general security guidelines, auditing, training, validation, and additional procedural and administrative controls.

When properly implemented, FactorySQL and FactoryPMI can help manufacturers in regulated industries achieve and maintain compliance. The bigger goal is to improve efficiency, simplify manufacturing, help with patent filing, and standardize your process.

21CFR11 is necessarily relevant to manufactures who submit their records to the FDA for review. Many guidelines represent "common sense" and "good practice" for manufacturers.

About this White Paper

The goal of this document is to describe how to use Inductive Automation software as a tool to help you develop 21CFR11 compliant applications. FactorySQL and FactoryPMI can be used to create compliant HMI/SCADA applications, but the software is not inherently compliant. 21CFR11 has as much to do with procedure, training, and even organizational culture as it does with software settings.

Regulations are given point by point as i*talicized text* followed by recommendations in normal text.

This document assumes that the customer is using a "closed system" as defined by **11.3(b)(4)**.

Where to get more information

Specific questions about FactorySQL and FactoryPMI will be answered on the Inductive Automation forum http://www.inductiveautomation.com/forum/
FDA requirement info http://www.fda.gov/ora/compliance_ref/part11/
An informative web site http://www.21cfrpart11.com

II. Background

In March of 1997, FDA issued final part 11 regulations that provide criteria for acceptance by FDA, under certain circumstances, of electronic records, electronic signatures, and handwritten signatures executed to electronic records as equivalent to paper records and handwritten signatures executed on paper. These regulations, which apply to all FDA program areas, were intended to permit the widest possible use of electronic technology, compatible with FDA's responsibility to protect the public health.

Subpart A – General Provisions
§ 11.1 Scope

11.1(a) *The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records, to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.*

11.1(b) *This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.*

11.1(c) *Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 20, 1997.*

11.1(d) *Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with § 11.2, unless paper records are specifically required.*

11.1(e) *Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.*

§ 11.2 Implementation.

11.2(a) *For records required to be maintained, but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.*

11.2(b) *For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that:*

11.2(b)(1) *The requirements of this part are met; and*

(2) *The document or parts of a document to be submitted have been identified in public docket No. 92S-0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.*

§ 11.3 Definitions.

11.3(a) *The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.*

11.3(b) *The following definitions of terms also apply to this part:*

11.3(b)(1) Act *means the Federal Food, Drug, and Cosmetic Act (secs. 201-903 (21 U.S.C. 301-393)).*

(2) Agency *means the Food and Drug Administration.*

(3) Biometrics *means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.*

(4) Closed system *means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.*

(5) Digital signature *means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.*

(6) Electronic record *means any combination of text, graphics, data, audio, pictorial or other information representation in digital form, that is created, modified, maintained, archived, retrieved or distributed by a computer system.*

(7) Electronic signature *means a computer data compilation of any symbol or series of symbols, executed, adopted or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.*

(8) Handwritten signature *means the scripted name or legal mark of an individual, handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.*

(9) Open system *means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.*

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:

11.10(a) *Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.*

It is the customer's responsibility to ensure system validation. Invalid or altered records can be discerned by the use of hash functions.

11.10(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.*

Historical data including alarm records and audit logs are maintained in a standard, vendor neutral, SQL compliant, relational database. FactoryPMI can be configured to present data in human readable forms such as pdf based reports, graphs, or tables. Inductive Automation recommends the use of open SQL database management tools for electronic access.

11.10(c) *Protection of records to enable their accurate and ready retrieval throughout the records retrieval period.*

It is the customer's responsibility to configure database security such that users cannot tamper with or remove data. SQL databases have the mechanisms and storage potential to make this possible. Customers are responsible for putting procedures in place to ensure data availability.

11.10(d) *Limiting system access to approved individuals.*

Limiting physical access is the responsibility of the customer. Inductive Automation recommends using Windows security via Active Directory to validate user access in FactoryPMI.

11.10(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.

Historical data records, alarm records, and FactoryPMI user audit logs are all stored in a relational database. Inductive Automation recommends that the application be set up such that only the system has permission to write to these tables. FactoryPMI should be configured to record operator actions via auditing. Most databases can be set up to maintain a detailed audit log of modification or deletion of such records modified outside of Inductive Automation software.

11.10(f) *Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.*

FactoryPMI contains tools for documenting every action taken by operators. Jython scripting can be used to ensure and enforce sequencing of steps and events. It is the responsibility of the customer to ensure these system checks are properly implemented.

11.10(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.*

It is the customer's responsibility to utilize Windows, SQL database, native FactoryPMI, and standard network security mechanisms to limit user access to assigned functionality and configure authentication properly.

11.10(h) *Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.*

FactoryPMI security can limit user access to assigned functionality. Jython scripting can be used to limit permission scope by node, user, or security group.

11.10(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.*

It is the responsibility of the customer to ensure that all individuals who develop, maintain or use the systems are qualified to perform their assigned tasks.

11.10(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.*

It is the responsibility of the customer to ensure that the policies are in place to hold individuals accountable for their actions.

11.10(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 timesequenced development and modification of systems documentation.*

Documentation control procedures are the responsibility of the customer. FactoryPMI supports electronic documentation in the form of pdf or html files stored in an SQL database and can be implemented with timesequenced revision control and access control.

§ 11.50 Signature manifestations

11.50(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*
(3) *The meaning (such as review, approval, responsibility, or authorship) associated with the signature*

FactoryPMI audit logs track the user and date and time when operator actions occur. Additional information may be stored in the SQL database on a per user or per electronic record basis.

11.50(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).*

The items identified in paragraphs **(a)(1)**, **(a)(2)**, and **(a)(3)** are stored in the same databases as mentioned in the above sections and therefore are subject to the same controls as for electronic records. It is the customer's responsibility to include the information as part of the human readable form.

§ 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.

Event records are maintained in a relational database and should utilize an audit trail to prevent falsification. Actual signatures (username and password) should be managed externally via Active Directory and a Microsoft Windows Domain.

Subpart C – Electronic Signatures
§ 11.100 General requirements

11.100(a) *Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.*

Inductive Automation recommends a strict security policy with Active Directory. Alternatively, FactoryPMI scripting and database security can be set up to ensure that all username and password combinations are unique and that signatures are not reused or reassigned.

11.100(b) *Before an organization establishes, assigns, certifies or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.*

Identity verification is the responsibility of the customer.

11.100(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.*

It is the customer's responsibility to 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.

(1) *The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.*
(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.*

It is the customer's responsibility to certify signatures and provide appropriate certification or testimony in accordance with FDA 21CFR11.

§ 11.200 Electronic signature components and controls

11.200(a) *electronic signatures that are not based upon biometrics shall:*

(1) *Employ at least two distinct identification components such as an identification code and password.*

FactoryPMI security utilizes a username and password combination.

(1)(i) *When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.*

(1)(ii) *When an individual executes one or more signings not performed during a single continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.*

Windows security or the FactoryPMI login requires the user to enter their username and password to gain access to the system. Jython scripting can be used to require additional password authentication to complete an action. Scripting can further be used to log users off after a defined period of inactivity using the **fpmi.system.getSecondsInactive()** function in a global timer script.

(2) *Be used only by their genuine owners*

It is the customer's responsibility to enforce the use of policies and procedures that ensure that the electronic signatures are only used by their genuine owners.

(3) *Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.*

Two person integrity is the responsibility of the customer. Windows security supports forcing users to change their passwords after being initially set by the administrator. Third party security applications may also be utilized.

11.200(b) *Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.*

It is up to the customer to select a third-party biometrics based mechanism for the system.

§ 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:

11.300(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.*

Windows security or SQL database security can enforce uniqueness of username and password.

11.300(b) *Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).*

Windows security includes password policies. It is the responsibility of the customer to ensure that the security policy is appropriate.

11.300(c) *Following loss management procedures to electronically de-authorize 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.*

It is the responsibility of the customer to implement loss management procedures to electronically de-authorize 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.

11.300(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.*

Windows security and/or third party applications can be configured to lock out accounts and report unauthorized activity to organizational management.

11.300(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.*

Device testing is the responsibility of the customer.

Total SCADA Freedom
2110 21st street suite 500
Sacramento, CA 95818
http://www.inductiveautomation.com