Application of the FDA 21 CFR Part 11 Standard at Rockwell Automation

Complying with 21 CFR Part 11: Electronic Records & Signatures

Regulatory Background

The law known as 21 CFR Part 11 was enacted in 1997 and updated in 2003, with a revision announced for 2006. However, that revision is still pending and may never take place, making the law more than 20 years old. To provide some context about when the law was written, dial-up was the typical internet connection, and the internet was still PG (pre-Google). Given its age, the law has been immune to the march of technology, providing requirements without being too prescriptive.

Most of the law requirements are now just considered good practice; they're what you'd reasonably expect from your system. None of the requirements are onerous or unreasonable, and some of them — like unique login credentials — are today seen as de rigueur.

Understanding the Regulations

21 CFR Part 11 is composed of two major subparts: electronic records and electronic signatures. These parts provide guidelines that regulated companies must minimally follow to achieve the level of integrity, reliability, and consistency of electronic records and signatures acceptable to the FDA. Complying with the Part 11 regulation requires a combination of strong management procedures and computer systems that meet the technical guidelines, including application security, audit trails and password protection.

Subpart A – General Provisions

The scope of this regulation is for any computer system producing electronic records intended to be the equivalent to handwritten records. Any Rockwell Automation application used to generate data as part of an electronic batch record for an FDA regulated product should be within the scope of this regulation.

Subpart A – Electronic Records

Section 11.10 – Controls for closed systems

Rockwell Automation applications are generally deployed as closed systems for use by System Owners, meaning the users of the system are responsible for the electronic records created and maintained in the system. It is critical that closed-system implementation and product capabilities work in conjunction to generate and maintain electronic records meeting the standards in Table 1. Electronic record systems that are closed must ensure the authenticity, integrity and, as needed, confidentiality of a record throughout its lifecycle.

System access must be tightly controlled using verification checks to confirm the users are authentic, trained and approved to use the system. System procedures should be in place to document how accesses to the system and electronic records are protected.

Table 1: Section 11.10

Requirements	Application Notes
11.10(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	System Owners are responsible for system validation, as it is unique in every implementation. Rockwell Automation can provide validation services for any validation activity performed during the specific integration of the system.
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.	All records are stored in SQL-compliant ODBC databases. Users can employ standard off-the-shelf or custom reporting tools to query the records in a human-readable form.
11.10(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	All records are stored in SQL-compliant ODBC databases and are available for viewing, printing, and exporting. System Owners are responsible for maintaining the electronic records per their retention period policy. System Owners are responsible for incorporating precautionary measures, such as periodic backup of the databases, into their policies. Access to these databases should only be provided to authorized users per System Owner policies to maintain data integrity.
11.10(d) Limiting system access to authorized individuals.	Rockwell Automation applications should use a combination of application and operating system security to limit access to authorized users. Additional security measures, such as limiting access to the operating system desktop, can be used to further restrict access.
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.	Rockwell Automation applications provide functionality to manage secure, computer-generated, time-stamped audit trails associated with operator actions performed in the production system.
11.10(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Rockwell Automation applications can provide controlled sequencing of manual and automatic steps and events. Additionally, operational checks, required by the System Owner can require security and authority checks to proceed.

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.	Rockwell Automation software uses a combination of operating system security and application security. System Owners are responsible for implementing policies and administrative procedures to define authorized access to the system. Rockwell Automation can aid in a security assessment and implementation for the system.
11.10(h) Use of device (for example, terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	Rockwell Automation applications use functions such as operator login and electronic signature to validate the source of data input. In certain cases, numeric entry controls provide minimum and maximum limits for data entry. The electronic signature can be configured to require the operator to reauthenticate (or both the operator and a member of a pre-configured approver group to reauthenticate) before completing the electronic signature. These functions should be included and configured per System Owner requirements. Rockwell Automation can provide consulting services to assess appropriate use of these functions.
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.	System Owners are responsible for hiring and training staff members with the education, training, and experience to perform assigned tasks. Rockwell Automation applications help support this requirement by validating that only users with appropriate security rights are granted access to the system.
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.	System Owners are responsible for implementing policies and procedures that outline the significance of electronic signatures in terms of individual responsibility and the consequences of falsification for both the company and the individual.
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 time-sequenced development and modification of systems documentation.	Rockwell Automation application user documentation is provided. The distribution of these documents is at System Owner discretion. A document management system can be used to manage deployed system documentation. (1) All Rockwell Automation documents are bundled and delivered with the product. Rockwell Automation assists with controlled delivery and distribution of the correct versioning of the documents. It is required that deployed system documentation be controlled and maintained for system operation and maintenance (2) Rockwell Automation assists with delivery and distribution of the correct versioning of the product documents. It is required that deployed system documentation be managed with proper revision and change control procedures.

Section 11.30 – Controls for open systems

Electronic record systems that are open must ensure the authenticity, integrity and, as needed, confidentiality of records throughout the record's lifecycle. Encryption and digital signature may be employed to facilitate this but are not prescribed. Access to Rockwell Automation applications require appropriate login and password, regardless of whether the System Owner chooses to implement a closed or an open system.

Table 2: Section 11.30

Requirements	Application Notes
11.30 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.	System Owners are responsible for establishing internal policies and procedures to put in place appropriate controls that meet regulations for an open system. Access to Rockwell Automation applications require appropriate login and password, regardless of whether System Owner chooses to implement a closed or open system.

Section 11.50 – Signature manifestations

When an electronic signature with an electronic record is presented, it must contain the name of the signer, date and time it was signed, and reason for signature (who, when and why).

Table 3: Section 11.50

Requirements	Application Notes
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; and (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	Within Rockwell Automation applications, electronic signatures captured in the audit trail include the name of the signer, operator ID, time and date stamp, and the action taken.
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).	Rockwell Automation audit log viewers show the user, time, and action. These fields are available for display or printout in any reports created using Rockwell Automation tools or a third-party tool.

Section 11.70 – Signature/record linking

When a signature, whether electronic or handwritten, is executed against an electronic record, it must be unalterable and unfalsifiable.

Table 4: Section 11.70

Requirements	Application Notes
11.70 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.	All records within Rockwell Automation applications are automatically tied to a specific user identity reflecting who performed each action. The records are stored in a compliant SQL database, but write access to the database should be secured to appropriate personnel.

Subpart A – Electronic Signatures

Electronic Signatures 11.100 – General requirements

Electronic signatures are intended to be equivalent to handwritten signatures, thus it shall have the proper mechanisms and controls in place to ensure it can be unique to one individual and no one else. Before assigning an electronic signature, it is necessary to confirm the identity of the individual and notify the FDA of the intent to use the electronic signature as legally binding.

Table 5: Section 11.100

Requirements	Application Notes
11.100(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	Rockwell Automation application security and operating system security meets this requirement by enabling the creation of a unique login and password for each user. System Owners are responsible for implementing procedures to ensure user IDs do not get deleted, reassigned or shared. It is recommended to disable user IDs rather than deleting them as a best practice for compliance reasons.

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.	System Owners are responsible for creating a management procedure that verifies the identity of an individual before sanctioning an individual's electronic signature. Once a user has been sanctioned and a unique account with password created in the system, the user is required to enter their login and password for access. This process validates the identity of the user in the system. These accounts can be created within Rockwell Automation applications or the operating system.
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. (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.	System Owners are responsible for notifying the FDA that they intend to recognize the electronic signature as a legally binding equivalent to traditional handwritten signatures. (1) System Owners are responsible for submitting certification to the FDA that the electronic signatures in their system are intended to be a legally binding equivalent to traditional handwritten signatures. (2) System Owners are responsible for any requested follow-up of certification or testimonial to have the electronic signatures be a legally binding equivalent to traditional handwritten signatures.

Electronic Signatures 11.200 – Electronic signature components and controls

Electronic signatures are typically administered non-biometrically (i.e., username and password), requiring application security to enforce appropriate policies that ensure only the assigned individual can execute the signature as needed and as many times as necessary. The execution of the electronic signature by someone other than that assigned individual must be restricted or managed appropriately. The use of biometrics can help ensure the electronic signature is only used by the assigned individual but must be designed to ensure it can meet the requirement.

Table 6: Section 11.200

Requirements	Application Notes
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. (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. (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. (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 its genuine owner requires collaboration of two or more individuals.	Rockwell Automation application security enforces unique user ID and password for each login credential and signature. System Owners are responsible for ensuring use of credentials by its genuine owner.
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.	Certain Rockwell Automation applications support biometric identification. See specific products for biometric support information. Biometric login identifiers are intended to, by design, be unique to an individual genuine owner.

Electronic Signatures 11.300 – Controls for identification codes/passwords

Proper controls are required to maintain the uniqueness of the username/password combination. Application-level security can be configured to require individuals to change their password after an extended period or to help prevent and report multiple unauthorized attempts to access a system. Devices, such as cards and tokens, can be used to generate identification information but must be periodically checked for altercation or falsification. In the event an individual has forgotten their username/password combination or lost their identification device, rigorous organizational procedures developed by the System Owner should be in place to handle the situation appropriately.

Table 7: Section 11.300

Requirements	Application Notes
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	Rockwell Automation application or operating system security can be used to manage user accounts. The application security or operating system security maintains all login IDs to help prevent reuse or reassignment of previously created login IDs.

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).	Rockwell Automation application or operating system security can be used to manage user accounts. Features provided by either approach include: password expiration, password aging, password complexity requirements, account expiration, disabling of accounts, lockout after invalid login attempts, and forcing a change of password on first login.
11.300(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.	System Owners are responsible for implementing loss-management procedures. If there is a lost device or compromised account, users can be deactivated.
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.	Rockwell Automation uses application or operating system security mechanisms to detect unauthorized use. Rules, such as a set number of false login attempts, can be configured. If attempts at unauthorized use is detected, it then locks the user account, preventing access and the ability to provide electronic signatures. An audit of all login attempts is recorded for historical tracking.
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.	System Owners are responsible for creating management procedures that include a periodic test of any devices that may risk the integrity of a user's identification.

Relationships Make Us Stronger

Since 21 CFR Part 11 was first enacted, Rockwell Automation has always supported our customers in meeting its requirements. We believe it is our duty to provide you with products that make it easy to fulfill your legal requirements. We are active in technical, industry, trade and legislative organizations to monitor current trends and best practices, as well as to ensure our products and services meet your needs now and in the future.

As part of these activities, we are active participants in the Parenteral Drug Association (PDA) Part 11 Task Group — an authority on Part 11 compliance. The PDA formed this task group to provide a set of best practices for complying with Part 11. The task group includes representatives from the pharmaceutical industry, suppliers, consultants and the FDA. Rockwell Automation is one of only two automation suppliers in this group. We have two members participating in the core group and two additional members on the extended team. This involvement gives Rockwell Automation direct access to accurate and up-to-date interpretations of the regulation and compliance practices as they evolve. These insights afford Rockwell Automation the opportunity to ensure its products and service can fully meet current best practices as understood by a multitude of critical stakeholders, most importantly those writing the regulations and those responsible for following them.

We also work with the life sciences industry to help provide confidence that our products comply with the technical aspect of Part 11. Each customer's security requirements and standard operating procedures (SOPs) for supporting this regulation are unique. Our products are flexible and configurable to meet the various SOPs and implementations needed to facilitate this regulation.

Our company also leverages its diverse industry expertise to apply best practices from one industry in another. For instance, when the original law was released, we leveraged disaster-recovery practices from the automotive industry and adapted them to others so the configuration of a controller was a manufacturing record, and changes required audit events and records.

We're here to help

Rockwell Automation designs its products and services from the ground up to provide a flexible and secure platform that enables you to automate your processes while meeting industry and legal requirements. We examine products from a risk perspective to ensure those with the greatest risks include functionality to mitigate it so customers can meet their production and legal requirements. Rockwell Automation has extensive experience helping our customer meet their goals. And our team brings the expertise to help guide you from original conceptualization through the entire automation lifecycle, including implementation, maintenance, migration and decommissioning.

This document describes our overall position regarding our product and service capabilities to meet the requirements of 21 CFR Part 11. The application notes in Tables 1-7 represent our recommendations regarding each paragraph of the CFR. More detailed information on specific product configuration or settings to meet the requirements can be found in specific product documents. However, the overall system of products should be considered holistically as a 21 CFR Part 11 solution. The complete system architecture — including robustness, data flow, security configuration and system management — will determine if compliance with 21 CFR part 11 is met.

Using our products, guidance documents and consulting services, Rockwell Automation is ready, willing and able to assist you in meeting the requirements of 21 CFR Part 11. Want to know more? Visit us at rockwellautomation.com.

Connect with us.

rockwellautomation.com — expanding **human possibility**®

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846