21 CFR Part 11 and Pharmaceutical Best Practices with Ignition

inductive automation

(800) 266-7798

inductiveautomation.com

Table of Contents

Introduction

Getting Started

Welcome to Inductive Automation's comprehensive guide on developing 21 CFR Part 11-compliant applications with Ignition. The Compliance Summary Table gives a brief overview of features included in Ignition and the scope of implementation that should be covered by an application's design in alignment with the company's policies. The Compliance Detailed Description gives specific guidance on how to comply with the spec. If you're new to Part 11, we recommend starting at the beginning of the guide to help you understand valuable background information and key concepts.

Background

Ignition by Inductive Automation

Ignition is regularly used in applications requiring 21 CFR Part 11 compliance by customers in the life sciences and pharmaceutical industries. Inductive Automation is committed to enabling customer success with regulated applications using modern technologies.

What is 21 CFR 11?

21 CFR Part 11 ("Part 11") is the established Food and Drug Administration ("FDA") regulation governing the use of "Electronic Records and Electronic Signatures" ("ERES"). The agency criteria outlines where electronic records and signatures can be substituted for paper records and handwritten signatures within FDA-regulated industries.

About This Guide

The purpose of this document is to provide industry-specific background information and show how compliant applications can be built with Ignition and standard technologies. It proposes a "shared responsibility" model between the customer, software vendors, and service providers.

Many Part 11 requirements can be satisfied with customer procedural and administrative controls, requiring few technical controls. However, it is a common pitfall to approach each requirement in isolation. This can lead to ineffective implementation decisions, such as considering security as an entirely "application layer" problem. Inductive Automation believes that the best way to succeed with Part 11 is to understand FDA guidance, adhere to industry best practices, and consider modern IT and OT technologies based on customer requirements and a risk assessment

backed by subject matter expertise. Modern external systems, such as Microsoft Azure AD for Identity and Access Management (IAM), offer strong security controls that clearly exceed Part 11 minimum requirements, but can also introduce new risks based on the reliance upon outside entities. The same concept applies to System Integrator and service provider deliverables. It is ultimately the customer's responsibility to meet Part 11 compliance and audit their vendors.

Convention

Font	Meaning
Italics	21 CFR 11 "Part 11" source or key terminology
Plain Text	Guide information or recommendation
Bold	Emphasized concept or category label
	**Additional Information**. Supplemental information often going beyond minimal Part 11 requirements.
	**Tip** or Industry Best Practice.
	**Ignition capability**. Configuration details or example implementation options.
	**Customer responsibility**. It may be possible to designate the activity to System Integrator, consultant, or Software as a Service (SaaS) provider. The customer should still be involved through oversight and auditing.
	**Customer choice**. Optional system or service to help satisfy requirements.

Industry Direction

Additional Information: Part 11 has not changed since 1997, but the FDA periodically releases "Guidance for Industry" (GFI). GFI is framed as "non-binding,"expressing the agency's "current thinking" on specific topics. For example, FDA guidance was released on "Part 11" in 2003, and on "Data Integrity and Compliance With [current good manufacturing practices] cGMP" in 2018.

The FDA and the industry maintain *Good Practices*, collectively referred to as "GxP." This guide incorporates FDA guidance, industry best practices, "lessons learned" from the Ignition community, and Information Technology and Operational Technology (IT/OT) methodologies covering the over-25-year

technology evolution gap between the original introduction of Part 11 and present day.

CDER and cGMP

Additional Information: The Center for Drug Evaluation and Research (CDER, "see-der") is a division of the FDA that regulates drugs. The FDA delegated primary Part 11 responsibility to CDER (FDA, Feb 2003). CDER enforces "Current Good Manufacturing Practice" (cGMP) regulations for drug manufacturing. cGMP does not specifically address Part 11.

FDA References

Tip: The FDA consistently lists the Good Automated Manufacturing Practices (GAMP) framework by the International Society for Pharmaceutical Engineering (ISPE) nonprofit organization under Industry References. GxP stakeholders should consider joining the ISPE and purchasing the latest GAMP material for direction.

ISPE

The International Society for Pharmaceutical Engineering (ISPE) is a nonprofit association serving its members by leading scientific, technical, and regulatory advancement throughout the entire pharmaceutical lifecycle.

GAMP

Tip: GAMP stands for *Good Automated Manufacturing Practices*, maintained by the *International Society for Pharmaceutical Engineering* (ISPE). GAMP 5 is both an ISPE subcommittee and set of guidelines applicable to the pharmaceutical and medical device industries. The 2nd edition of GAMP 5, released in July 2022, incorporates FDA guidance and current industry best practices. "GAMP is not a prescriptive method or standard, but rather provides pragmatic guidance, approaches, and tools for the practitioner. When applied with experience and good judgment, the guide offers a robust, cost-effective approach" (ISPE, GAMP 5 introduction). GAMP provides practical guidance to facilitate interpretation of regulatory requirements.

Key Concepts

Data Integrity

Integrity as a principle refers to data trustworthiness and reliability in the context of protection from unauthorized changes and attribution. Integrity is an important aspect of Part 11 compliance with Electronic Records and Electronic Signatures.

ALCOA+

Additional Information: "Data integrity refers to the completeness, consistency, and accuracy of data. Complete, consistent, and accurate data should be attributable, legible, contemporaneously recorded, original or a true copy, and accurate (ALCOA)." (FDA, 2018). ALCOA has since been expanded to ALCOA+ (WHO and GAMP 5) to include "available, enduring, consistent, and complete".

Database Systems

Commercial database systems include mature data integrity and ALCOA+ features. Part 11 systems often rely on OT- or IT-managed database systems from Microsoft, Oracle, and other vendors hosted either on-premise or in the cloud.

Tip: GAMP 5 (section 48.2.5) recognizes that GxP regulated databases used for data audit trails may require external controls. Proprietary and open-source "desktop databases" are noted as often being less secure than IT-managed server-based environments. While not explicitly specified, this is understood to be local products such as Microsoft Access or equivalent. Spreadsheets are discussed for use as calculators or retention as documents and not recommended for use as "databases." A "best practice" is to inherit security controls from properly configured, IT-managed, enterprise or cloud database systems. GAMP 5 and the FDA mention "Oracle."

Shared Responsibility Model

This guide proposes that the customer, their vendors, and optionally, their service providers each have responsibilities to achieve success with Part 11-compliant projects.

Customer

Customer responsibility: The customer is ultimately responsible for compliance. The customer will have flexibility in deciding between *Operational and Administrative Controls* (executed by people as opposed to systems) and

Technical Controls (implemented through hardware or software). Customers often rely on System Integrators to help achieve compliance.

Customers should minimally:

- Maintain policies and procedures that hold users accountable, developed in accordance with a risk-based approach
- Address how vendors are assessed
- Provide training
- Enforce change control
- Perform validation

It is the customer's responsibility to audit vendors and service providers to ensure that requirements are being met and compliance is maintained.

Software Vendor

Ignition capability: Part 11 applications characteristically integrate multiple hardware and software products within a defined environment. Vendors should demonstrate how they, as part of the critical supply chain, adhere to best practices with quality and security. Vendors should also provide recommendations for using their software in a Part 11 environment including configuration recommendations. Ignition is well suited for Part 11 applications and can be used for: process real-time status and control, alarming, reporting, user auditing, and more. This guide speaks to "best practices" using Ignition as an integrated platform within a customer's designated IT/OT environment to best achieve Part 11 compliance.

Consultants or System Integrators

Customer choice: Consultants or System Integrators (SIs) may offer Part 11-compliant implementation services using Ignition and other hardware or software products. Some may provide services such as qualification testing, user training, and procedure templates to help customers navigate the compliance process.

Inductive Automation maintains a listing of over 2,700 Integrators worldwide and provides certification standards. Please contact your account representative for specific SI references. https://www.inductiveautomation.com/integrators/

Cloud Service Providers

Customer choice: Cloud Service Providers (CSP) include best practices for running Part 11-compliant or similar applications within their infrastructure. These

tend to provide a high level of validated assurance “lower in the stack” and leave the application portion (where Ignition resides as a SCADA system) to the customer. Amazon provides 21 CFR 11 Best Practices and an AWS Config Guide. Microsoft hosts a 21CFR11 portal and provides Azure GxP Guidelines. Google provides GxP and 21 CFR Part 11 guidance.

Tip: CSPs offer virtual networks, which are isolated customer environments that can be interconnected with customer infrastructure through secure connections including “cloud peering” without the public Internet. Ignition supports “n-tiered” architectures and most secure remote access technologies.

Software/Platform as a Service (SaaS/PaaS)

Customer choice: Software- and Platform-as-a-Service (SaaS/PaaS) models provide customer options where vendors can assume greater Part 11 responsibility based on managing infrastructure that processes customer data. Service providers are able to perform compliance activities, such as computer system validation, change control, process automation, and user training. SaaS/PaaS offerings enable a high degree of inherited assurance through architecture and service automation (orchestration of “the technology stack”), greatly exceeding what is feasible with most on-premise environments. SaaS/PaaS Part 11 offerings will all require custom integration, but are likely as close to “turnkey” as possible with many project aspects. SIs should be able to help with SaaS/PaaS offerings. The customer should plan on regularly auditing SaaS and PaaS providers.

Tip: It is a natural fit for SaaS/PaaS Part 11 service providers to offer customers dedicated VPCs running on the “big name” CSPs (e.g. AWS, Azure, GCP) configured in accordance with best practices. Secure interconnects and web services technologies provide safe options to access shared services.

Ignition Best Practices

Tip: Following Ignition best practices simplifies the validation process by demonstrating high levels of assurance with electronic records and electronic signatures. Part 11 compliance does not depend on any specific technology or configuration. This guide recommends a risk-based decision-making approach based on customer requirements and industry standards, backed by subject matter expertise.

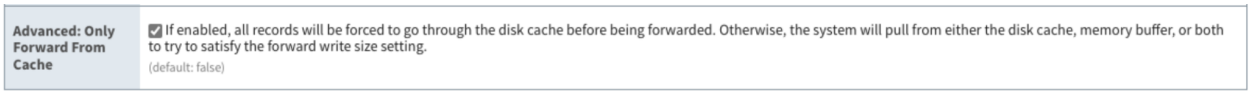
Inductive Automation provides a Security Hardening Guide and a Server Sizing and Architecture Guide to assist with best practices. The following recommendations align with the intent of Part 11 and GxP best practices.

1. Use an external Identity Source for user authentication (verifying identity) and authorization (managing access rights). This could be an on-premise Enterprise system such as Microsoft Active Directory or a third-party Identity Provider (IdP), which can be locally managed or provided by a cloud service. Local OS or application managed user accounts are generally weaker and not recommended for Part 11 applications. The most secure and realistic options will require strong or multi-factor authentication for all users through an identity and access management service, which can be local, cloud-hosted, or a hybrid of the two.
    i. Assign Ignition roles based on IdP groups, such as Active Directory Groups.
    ii. The most current Microsoft approach uses Azure AD (Entra). On-premise solutions are possible such as Apache Keycloak, Red Hat Identity Manager, or HashiCorp Vault. Third-party solutions such as: Duo, Okta, Ping, offer powerful hybrids. Enterprise solutions are offered from Oracle, IBM, RSA, Symantec (Broadcom), and others.
2. Follow the Ignition Security Hardening Guide for security best practices with Ignition and the immediate computing environment. Include supporting IT and OT departments from the start. They likely have people, processes, and tools to help. From the Ignition Security Hardening Guide:
    i. Consider a foundational model and strategy. “Zero Trust,” “Defense in Depth,” “Zones and Conduits,” and “Purdue Model” are examples. Align with organizational best practices.
    ii. Force secure client communication with Ignition using HTTPS with genuine TLS certificates. Employ “strong headers” with HSTS redirects and consider disabling older cipher suites.
    iii. Follow Identity and Access guidance. This includes using secure LDAP (LDAPS) for Active Directory connections and SAML or OpenID Connect for Identity Providers. Adhere to your organizational policy on account usage and lifecycle.
    iv. Consider additional authentication factors. Role-Based Security is a great starting point. Ignition supports additional features such as location, security zones, and security levels. Identity providers are moving in the direction of pattern of use, device health checks, and other non-traditional factors.
    v. Apply good cybersecurity hygiene. Remove unnecessary applications, lock down the host operating system, keep systems up to date, and stay consistent with organizational best practices. This might include the IT or OT department maintaining endpoint protection systems.
3. Extra consideration of database protections is warranted for Part 11 applications.

i. Discuss the best options with IT, OT, and cybersecurity stakeholders.
ii. Configure dedicated Ignition database connections for the project, Audit Log, and Historian. Apply separate credentials for each. Apply best practices for security controls and auditing consistent with company policy, vendor recommendations, and project risk analysis. For example, grant SELECT and INSERT (not UPDATE or DELETE) on an audit schema.

Name	Description
Application	Custom database available for project use
AuditLog	Append-only database connection for audit log
Historian	Append-only database connection optimized for time-series data

iii. Force disk cache usage for database interactions. Forcing disk cache usage preserves records in the event of a power outage where records have not yet been written to a database or store-and-forward cache. Additional mitigation is possible with environmental controls such as local UPS and fuel-based generator support.



4. **Architecture**. It may be appropriate to start with a single Ignition Gateway. However, Ignition "scale-out" architectures offer improved security, performance, and survivability characteristics. Follow the Server Sizing and Architecture Guide when scaling out.

Tip: Secure architectures are possible using Ignition gateways to apply the *Principle of Least Privilege* with network segmentation. The concept is that most nodes (e.g. clients, databases, network and OT devices) can only communicate within a zone, preferably only to the nearest Ignition gateway. Ignition gateways relay traffic by securely inter-communicating between zones using secure "Gateway Network" (GWN) or MQTT connections ("conduits") with certificate-based, secure TLS connections over a single TCP port. External firewalls are recommended between zones.

Tip: "Stateless" *frontend* (aka "*visualization*") gateways run projects and communicate securely with Ignition clients, often through a load balancer. "*I/O*" gateways maintain "state", which includes the tag system, script and logic execution, device, and database connections. I/O gateways can be protected with Ignition Redundancy where a secondary Gateway is ready to take over. "Edge" devices running Ignition offer proximity advantage. In the event of a network or

server failure, local control is possible with Edge devices. A “store-and-forward” buffer retains historical data. Many legacy OT protocols used to communicate with industrial control systems are inherently weak. Ignition Edge allows segmentation in accordance with best practices such as ISA/IEC 62443 “Zones and Conduits” or ISA-95 “Purdue Model” segmentation. This is typically accomplished with network segmentation (dividing) and segregation (controlling communication) such as VLAN and VPN technologies.

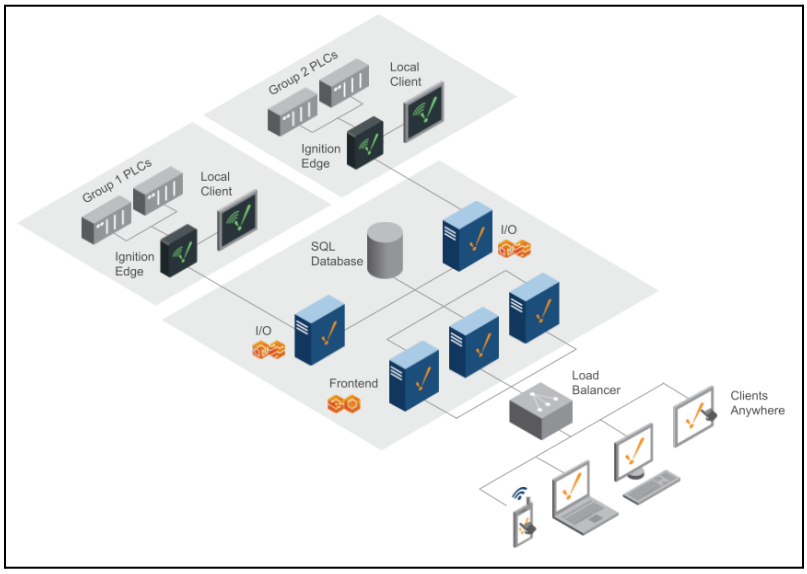


Figure 1. Reference: Scale-out architecture example

5. **2-Person Integrity**.

Ignition capability: Ignition provides *system.security.validateUser* and system.perspective.authenticationChallenge scripting functions to allow in-session 2-person integrity checks such as the Done-By/Checked-By examples below. This can be used to satisfy § 11.200(a)(3), misuse requiring collaboration by 2 or more persons, as well as enhance capabilities supporting multiple *Electronic Record* and *Electronic Signature* requirements.

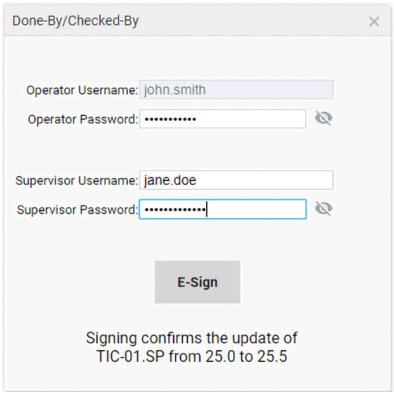


Figure 2. Done-By/Checked-By with 2-person integrity using Microsoft Active Directory

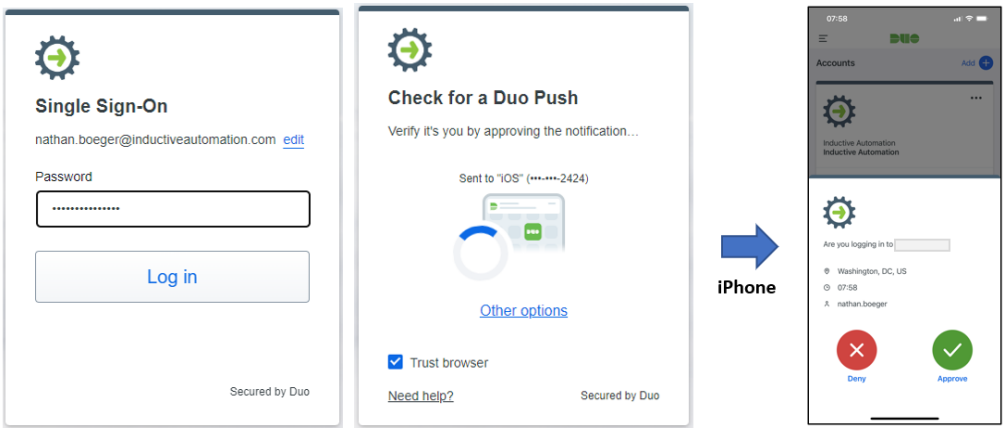


Figure 3. Example: IA uses On-Prem Active Directory + a Duo mobile device push

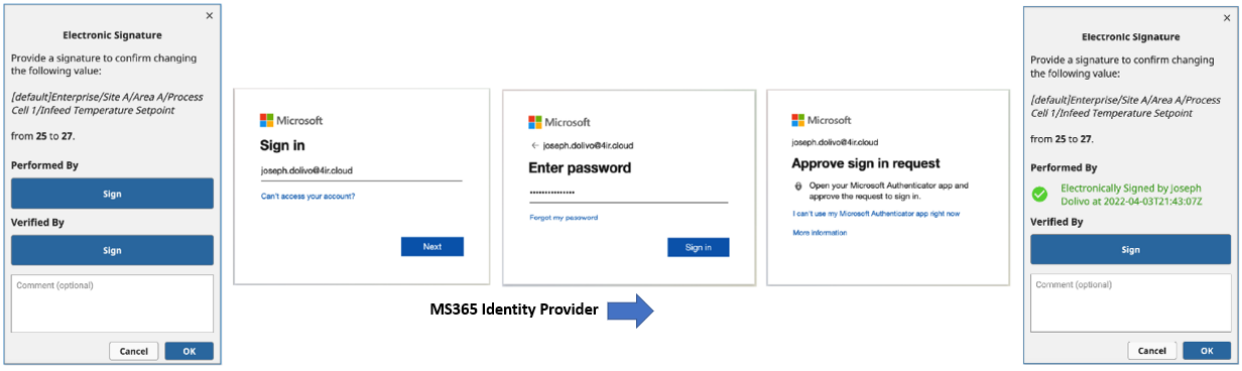


Figure 4. Example of Done-By/Checked-By using O365 with MS Authenticator App

21 CFR Part 11 Compliance

Compliance Summary Table

Part 11 Requirement (IA Summary)	Notes
Subpart A - *General Provisions*	Outlines: scope, implementation, definitions
Subpart B - *Electronic Records*	
§ 11.10 Controls for closed systems	
a. Validation	Customer. See Validation and Qualification and FDA Guidance For Industry.
b. Record generation	External databases with append-only permissions
c. Record protection	External databases with append-only permissions. For more information, see FDA Guidance For Industry.
d. Limiting system access	Role-based access; timed user logout
e. Digital audit trails	Use append-only write credentials
f. Permitted sequencing of steps and events	Ignition SFC Module, Sepasoft Batch Procedure Module, or scripting
g. Authority checks	Follow best practices; Perform audit reviews of successful and failed logins, and logouts. Follow local policies such as locking of accounts on multiple failed logins, minimum password length and strength, etc.
h. Device checks to validate data input or operational instruction	Multiple mechanisms
i. Training and qualification	Customer. IA can validate Ignition certification status supporting customer training audits on system integrators. IA offers comprehensive free training resources.
j. Written policies	Customer. GAMP 5 offers best practices
k. Documented controls	Customer. (GAMP 5 Guidelines section 16.3, 17)

1. Operation and maintenance 2. Change control	Configuration and Change Management, Documentation and Information Management. Ignition supports formal “Source Control” systems.
§ 11.30 Controls for closed systems	Customer decision for “Open” or “Closed” system. Best practices offered to achieve an “Open” system.
§ 11.50 Signature Manifestations	Ignition supports with customization
a. Signed electronic records	
1. Printed name	
2. Date and time	
3. Meaning associated	
b. Inclusion (display, printout)	
§ 11.70 Controls for closed systems	Ignition best practices satisfy requirements
Subpart C - *Electronic Signatures*	
§ 11.100 General requirements	
a. Unique signatures	Inherited by following best practices
b. Identity verification	Customer activity when issuing accounts
c. Signature certification	Customer procedural responsibility with FDA.
1. Certification submission	
2. Nonrepudiation	
§ 11.200 Components and controls	Inherited by following best practices
a. Non-biometric signatures	
1. Factor / components	
i. Multiple signatures	Ignition implementation
ii. Noncontinuous signatures	Ignition implementation
2. Genuine owner	Inherited by following best practices
3. 2-person integrity	Supported by Ignition features
b. Biometrics	Optional; possible through Identity Providers
§ 11.300 id codes and passwords	Ignition provides
a. Uniqueness	

b. Lifecycle	Inherited by following best practices
c. Loss management	Inherited by following best practices
d. Transaction safeguards	Inherited by following best practices
e. Testing	Inherited by following best practices

Compliance Detailed Description

Subpart A - General Provisions

§ 11.1 Scope. See source.

§ 11.2 Implementation. See source.

§ 11.3 Definitions.

(1) ***Act*** *means the Federal Food, Drug, and Cosmetic Act (secs. 201-903 (21 U.S.C. 321-393)).*

(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:

The agency expects consistent organizational procedures and controls. The Good Automated Manufacturing Practice (GAMP) 5 framework, maintained by the International Society for Pharmaceutical Engineering (ISPE), provides a lifecycle model and a great optional starting point. From a data security perspective, achieving a high degree of confidence in the principle of "integrity" is needed to trust records as genuine and achieve nonrepudiation.

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

Customer responsibility: System validation is a **customer responsibility** that should be performed by an independent department or outside entity to avoid conflict of interest. The customer should track and audit results, even if validation work is performed by contractors or service providers. See Appendix D for *validation* information.

Updated FDA guidance (2003 Guidance to Industry on Part 11 Scope and Application)

> The Agency intends to exercise enforcement discretion regarding specific Part 11 requirements for validation of computerized systems (§ 11.10(a) and corresponding requirements in § 11.30). Although persons must still comply with all applicable predicate rule requirements for validation (e.g., 21 CFR 820.70(i)), this guidance should not be read to impose any additional requirements for validation.
>
> We suggest that your decision to validate computerized systems, and the extent of the validation, take into account the impact the systems have on your ability to meet predicate rule requirements. You should also consider the impact those systems might have on the accuracy, reliability, integrity, availability, and authenticity of required records and signatures. Even if there is no predicate rule requirement to validate a system, in some instances it may still be important to validate the system.
>
> We recommend that you base your approach on a justified and documented risk assessment and a determination of the potential of the system to affect product quality and safety, and record integrity. For instance, validation would not be important for a word processor used only to generate SOPs.
>
> For further guidance on validation of computerized systems, see FDA's guidance for industry and FDA staff General Principles of Software Validation and also industry guidance such as the GAMP 4 Guide.

Note: 21 CFR 820.70(i) falls under subchapter H (Medical Devices). The most recent GAMP guide is GAMP 5 second edition, released July 2022.

The FDA *General Principles of Software Validation; Guidance for Industry and FDA Staff* (FDA, Jan 2002) addresses software validation in detail. Inductive Automation generally adheres to these principles for Ignition development (Appendix F, SDLC), including maintaining a dedicated quality assurance department. The FDA guide recognizes that some responsibility can be transferred to the off-the-shelf software vendor. In this context, the full FDA guidance for software validation goes above and beyond the Part 11-applicable application features. The document references use cases such as validating embedded firmware in medical devices. However, the same principles can be applied for system validation on a more limited scale to achieve Part 11 compliance.

Tip: GAMP 5 (optional) provides a modern framework for computer system validation that accounts for: impact, complexity, and novelty of the solution (i.e. risk on product quality, patient safety, and record integrity). The GAMP 5 Appendix M1 discusses a validation strategy based on risk assessment, lifecycle model, inputs and outputs, acceptance criteria (e.g. Minimum Viable Product (MVP) and Definition of Done (DoD)), traceability, design review, and other functions. Appendix M7 covers validation reporting. ISPE offers targeted resources such as the Good Process Guide: Process Validation (ISPE, 2019).

Ignition capability: Ignition, like most SCADA packages, is a Category 4 software package according to GAMP. Scripting and custom queries are considered to be Category 5. Ignition supports the GAMP lifecycle approach with formal version control system integration (e.g. Git).

Tip: Software validation, which the FDA and GAMP refer to as “requirements traceability,” can either be achieved externally, with Ignition through customization, or via third-party tools such as Kneat or Confluence & Jira (with added plugins).

Tip: ***The ability to discern invalid or altered records***. Database systems such as SQL Server and Oracle have the ability to run “triggers”, which execute code on a database action. It is possible to add a *lastModified* field to a database table and create database triggers that update this value. Invalid or altered records could be discerned by a query that compares the record value to the *lastModified* value. Additionally, the trigger could log extra information to a different table. Consider that the Ignition account for logging data is recommended as append-only

(SELECT and INSERT, not UPDATE or DELETE), which further mitigates record alteration. Database systems include native and third-party tools (i.e. ApexSQL Audit) to help assure record integrity. External read-only database backups can help adjudicate cases with suspected invalid or altered records.

(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.

Ignition capability: Ignition stores historical data including alarm records and audit logs in standard, vendor neutral, relational databases. Microsoft SQL Server and Oracle are popular database products for GxP applications. Ignition can be configured to present data in human-readable and printable forms such as pdf-based reports, graphs, or tables. Inductive Automation recommends the use of standard SQL database management tools.

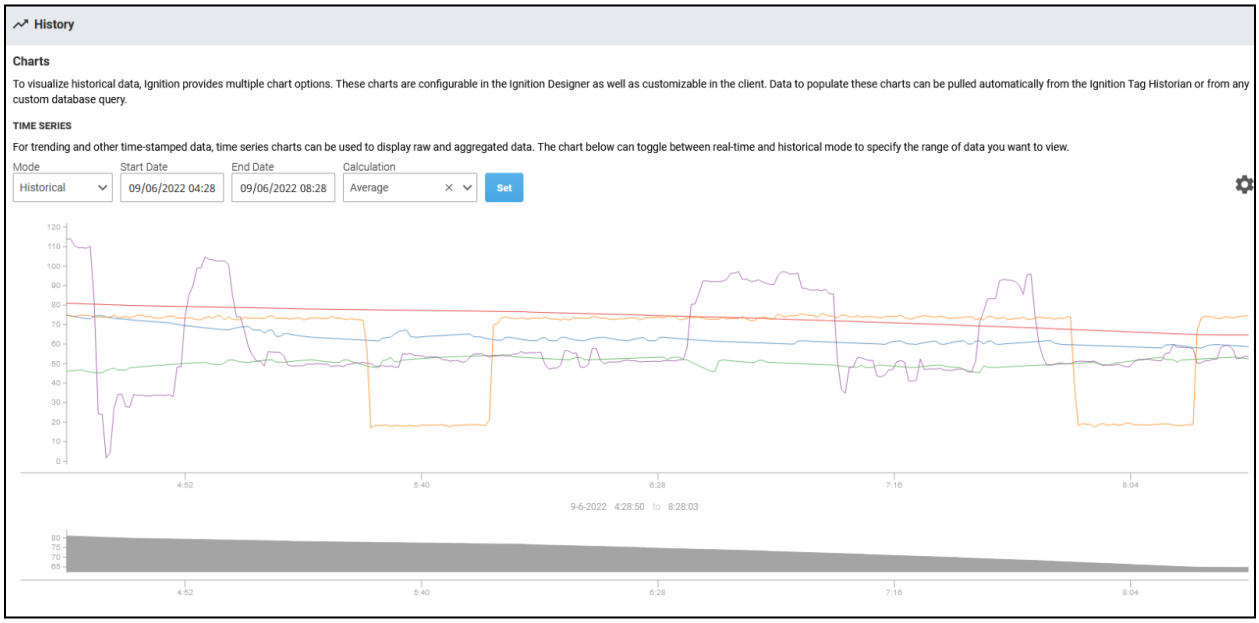


Figure 5: Example: Configurable and flexible charts to present historical/runtime process data

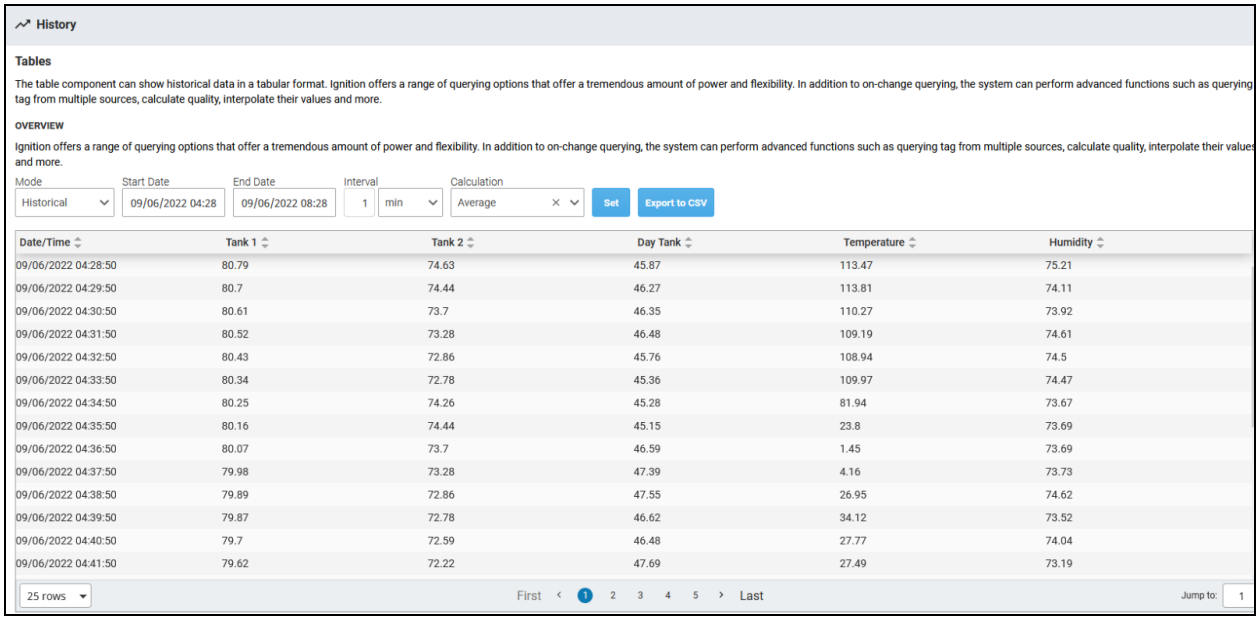


Figure 6: Example: Configurable and flexible tables to present historical/runtime process data

Note: “Complete copies of records” has long-term data archival and retrieval implications. FDA Part 11 Guidance for Industry addressed this common customer concern in 2003. “The Agency intends to exercise enforcement discretion with regard to specific Part 11 requirements for generating copies of records (§ 11.10 (b) and any corresponding requirement in §11.30).”

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

Tip: The use of properly configured and managed, standard relational databases, with access configured according to the Principle of Least Privilege ensures an adequate degree of record protection. Regular database backups are part of good cyber hygiene.

Customer responsibility: It is a procedural option for customers to maintain derivative copies of records for ready retrieval. For example, all data throughout the records retention period is stored in database tables. Ignition is capable of specific exports to spreadsheet, document, pdf, or print format.

Tip: Cloud-based tools can make it easy to archive or present “live” data to the agency as needed.

Updated FDA guidance (2003 Guidance to Industry on Part 11 Scope and Application)

The Agency intends to exercise enforcement discretion with regard to the Part 11 requirements for the protection of records to enable their accurate and ready retrieval throughout the records retention period (§ 11.10 (c) and any corresponding requirement in §11.30). Persons must still comply with all applicable predicate rule requirements for record retention and availability (e.g., §§ 211.180(c),(d), 108.25(g), and 108.35(h)).

We suggest that your decision on how to maintain records be based on predicate rule requirements and that you base your decision on a justified and documented risk assessment and a determination of the value of the records over time.

FDA does not intend to object if you decide to archive required records in electronic format to nonelectronic media such as microfilm, microfiche, and paper, or to a standard electronic file format (examples of such formats include, but are not limited to, PDF, XML, or SGML). Persons must still comply with all predicate rule requirements, and the records themselves and any copies of the required records should preserve their content and meaning. As long as predicate rule requirements are fully satisfied and the content and meaning of the records are preserved and archived, you can delete the electronic version of the records. In addition, paper and electronic record and signature components can co-exist (i.e., a hybrid situation) as long as predicate rule requirements are met and the content and meaning of those records are preserved.

(d) Limiting system access to authorized individuals.

Ignition capability: Ignition Role-Based Access Control (RBAC) ensures that system access is limited to authorized users. Best practices assure a high degree of trust throughout the lifecycle including access, user management, and auditing. Organizational procedures are required to verify individuals against accounts, provide physical security, surveillance, and other controls to demonstrate compliance.

Tip: Ignition is capable of automatically logging users off or locking the application after an organization-defined period of inactivity. Multi-factor authentication significantly reduces the risk of user credential sharing.

(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.

Ignition capability: Ignition audit logs generate time-stamped audit trails that independently record all user activity including operator entries. All audit entries are append entries. The best practice is for the audit profile database account to have (SELECT and INSERT) not (UPDATE or DELETE) permissions to the audit database. Audit logs are small enough files that modern database systems can be configured to maintain logs throughout the record retention period. Logs can be

exported in a variety of formats to satisfy agency review and copying requirements.

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

Ignition capability: Ignition can enforce permitted sequencing of steps and events. Workflows are flexible in terms of user steps such as reviews, approvals, justification, and other actions. The recommended approach uses the Ignition SFC Module or the Sepasoft Batch Procedure Module, both considered GAMP software Category 4 - "Configured Components." Customization is also possible through Python scripting, considered GAMP software Category 5 - "Custom Applications and Components." See figures below.

Tip: Operational system checks can include external input such as PLC controller logic, input from business systems such as via REST API, or user input. Operational checks should be tracked and verified during validation.

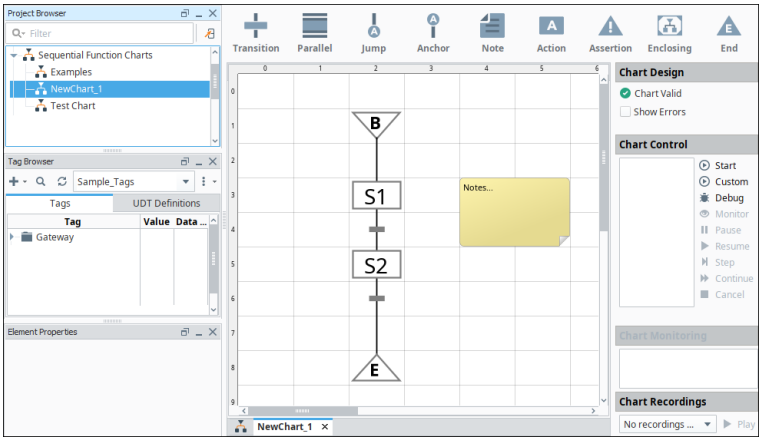


Figure 7. Example: Sequenced Logic flow with Ignition Sequential Function Chart

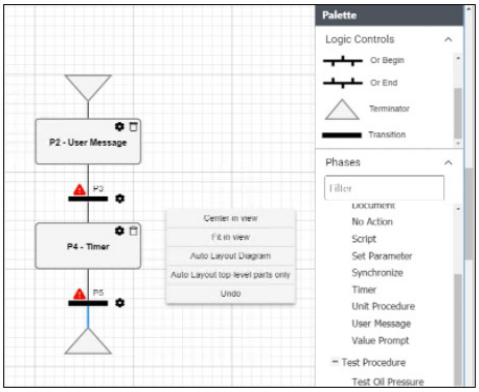


Figure 8. Example: Sequenced Logic flow with Sepasoft Batch Procedure Module

(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.

Tip: When following best practices, Ignition provides a high degree of assurance that system access, electronic signatures, record alteration, and operations are conducted by authorized individuals. The customer may validate.

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

Tip: Ignition offers several means to validate data input or operational instruction at multiple levels. Graphical components support input bounds and rules, which can be dynamic. Scripts can perform operations on sets of data, such as entire forms being submitted or workflows. Similar checks are possible at the database layer or OT device layer.

(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.

Customer responsibility: User education, training, and experience is a customer responsibility. GAMP 5 section 6.1.3 provides training process recommendations for computerized systems and scope. System Integrators or SaaS providers may be able to assist with training, material, and documentation.

Inductive Automation is committed to helping customers be successful with Ignition.

- Inductive University offers free training.

- Webinars offer Ignition guidance and examples.
- In-Person and Live Virtual Training help customers succeed.
- Ignition Certification is offered for System Integrators and users.

Tip: Customers may ask Inductive Automation account representatives for Ignition training or certification records for System Integrators (SI) who develop, implement, or maintain the Ignition system as part of a supplier audit. It is recommended to set qualification and auditing expectations with partners including SIs early in the project lifecycle.

(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.

Customer responsibility: Written policies and policy enforcement are a customer responsibility. System Integrators or SaaS providers may be able to assist with example policies that have successfully been used in other Part 11-compliant and validated applications.

Tip: GAMP 5 section 6 provides recommendations for establishing governance (e.g. policies & procedures, roles & responsibilities, training, supplier relationships, maintaining a system inventory, plan for validation, continual improvement, and data governance). Section 6.1.1 recommends policy commitments for *Computerized Systems Policies and Procedures*.

(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.

Customer responsibility: Documentation management is a customer responsibility. System Integrators or SaaS providers may be able to assist. Many customers choose to use complementary external packages such as corporate portals. Packages such as Confluence or Kneat also provide powerful options.

Ignition capability: Ignition supports formal “source control” systems such as “Git” (Ignition 8 Deployment Best Practices Guide) for SCADA configuration management. These systems allow collaboration, change tracking with revision history, reverting to previous versions, and troubleshooting throughout the project lifecycle. Source control systems can be used for DevOps or document

management outside of Ignition. Documentation is possible within Ignition with native components, customization, or optionally with the Sepasoft Document Management Module.

Tip: GAMP 5 suggests that automated tools offer significant advantages and that "selection, verification, and use of such tools should be documented and based on risk, complexity, and novelty". A source control system may be appropriate. Ignition is capable of tracking these items through customization, but dedicated tools will likely provide a better fit.

GAMP 5 Guidelines section 16.3 (Configuration and Change Management) and 17 (Documentation and Information Management) cover best practices for GxP computerized systems.

Configuration management. Track state and changes to all components of a computerized system. Configuration is documented throughout the lifecycle including *identification* (what), *control* (how), *status accounting* (how to document), and *evaluation* (how to verify).

Change management. Change management is an important process to track and document: project changes, planning docs, vendor contracts, requirements, design specifications, quality review, risk assessments, test reports, HW, software, and configuration. Inductive Automation recommends using formal source control systems (e.g. Git) to track Ignition project changes and enterprise tools for GAMP document management for Part 11 applications.

*§ 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.

Customer responsibility: Managing access permissions is a customer decision. Ignition is regularly used to achieve high levels of assurance. Controls for "Open Systems" depend on the entire environment and integrating well. Most SCADA vendors claim Part 11 applicability to "Closed Systems" only. "Open Systems" are defined as "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." This could be on-premise, cloud, or hybrid. The FDA offers little specific guidance on what constitutes "appropriate additional measures." This guide recommends following best practices especially adhering to current: vendor specific, NIST, and

CISA recommendations. The best approaches are likely to implement security frameworks (e.g. NIST CSF, ISA/IEC 62443, or CIS v8) and use strong Identity and Access Management (IAM) systems with multi-factor authentication and modern techniques. Success is likely a joint effort with organizational IT, OT, and cybersecurity teams. System Integrators can help. SaaS providers are likely a good option due to offering enhanced security controls through architecture automation and security services. For example, if the customer chose to host in an AWS or Microsoft Azure environment, the recommendation is to use a dedicated virtual private cloud (VPC) and adhere to the AWS or Azure Well-Architected Framework. Environment tools and services exist to achieve a high degree of confidence in record authenticity, integrity, and confidentiality. Inductive Automation hosts an internet accessible public demo running "off the shelf" builds of Ignition at: https://demo.ia.io that demonstrates a reference "scale-out" architecture over multiple cloud regions and availability zones. The system is maintained following the same guidelines outlined here.

Tip: Encryption of all data in transit is a requirement for open systems. This is best achieved with industry standard technologies such as mandatory enforcement of https with TLS 1.2 or 1.3 using genuine certificates.

§ 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.
(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).

Ignition capability: Ignition audit logs include the printed name and a date and time in a timezone agnostic format. The signature meaning (such as review, approval, responsibility, or authorship) can be captured through the use of a drop-down list along with free-form notes to be associated with the electronic signature. It is possible to display old and new values and 2-person integrity through the "Done-By/Checked-By" methodology (Ignition best practice #5 above).

Figure 9: Audit-Trail example including: date/time, action, old and new value, 2-person integrity, and failed attempts.

§ 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.

Ignition capability: Inherited based on best practices. Records are written by the system with append-only permissions to a protected database system. Signatures include the unique identifier of the signer. There is no way to falsify an electronic record by ordinary means.

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.

Ignition capability: Inherited. Signatures are associated with user accounts, which are unique. It is up to organizational policy to prevent behavioral reuse or misuse. Multi-factor authentication makes reuse or misuse much more difficult.

(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.

Customer responsibility: The customer should validate individual identity and assigned roles prior to granting account access. This is usually done in conjunction with signing organizational acceptable use policies.

(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.

Customer responsibility: This requirement is entirely between the customer and the FDA.

§ 11.200 Electronic signature components and controls.
(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.

Ignition capability: Inherited. Part 11 Ignition applications are recommended to use an external user source such as Microsoft Active Directory that minimally requires a distinct login and password. Requiring an additional factor such as token, device, or Authenticator app is highly recommended.

(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.

Ignition capability: Authentication for electronic signatures is flexible with Ignition. Multiple signature actions can be combined through user-configurable scripting with access to external Identity Providers.

(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.

Ignition capability: Ignition can be configured to require all electronic signature components prior to the first action. Logical timeouts or logouts can be used. Ignition is capable of 2-person integrity, requiring two people to authenticate for

designated actions. Authentication could be done by both parties on the same screen, or separately through a process workflow.

(2) Be used only by their genuine owners; and

Ignition capability: Inherited by design. Identity systems provide a high degree of assurance of the authenticity of the genuine owners, especially when employing multi-factor authentication. Organizational policies on account lifecycle, such as verifying individuals against accounts and diligently removing access upon transfer or termination, demonstrate additional assurance.

(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.

Ignition capability: Ignition provides the capability to enforce 2-person integrity for electronic signature actions using the system.security.validateUser function with Active Directory or system.perspective.authentiationChallenge function to challenge an Identity Provider (see reference). In Ignition best practice #6, see 2-person integrity “Done-By/Checked-By” examples using on-premise Active Directory and with federated Identity Providers.

Tip: Technical Note. It is difficult and inconvenient to prevent individual system administrators entrusted with elevated privileges from being able to reset and use multiple user accounts. Privileged Access Management (PAM) solutions might help. Customers should address this in policy with administrative controls. Inductive Automation recommends the practice of “segregation of duties” between privileged users, account requestors, data owners, and other key roles. Mitigating technical controls include: write-only auditing, logging to other systems, notification, and a review process. Privileged activities should be recorded such that unauthorized usage is obvious to other system administrators or internal oversight. This forces undetected unauthorized access to require collaboration of two or more individuals with elevated system privileges. Maturing Identity and Access Management (IAM) systems are moving in the direction of AI/ML enabled policy engines, workflows, time-based credentials, and separating roles to address the unlimited capability of legacy “admin” or “root” roles. Multi-factor authentication with company equipment and device checks also helps. Ignition supports these with federated identity providers.

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

Ignition capability: Inherited by design. Identity providers featuring biometrics offer high assurance that authentication only works with genuine owners. These integrate options like TouchID and FaceID APIs on iOS/MacOS and Android's fingerprint feature.

Tip: Modern examples. Microsoft AzureAD supports passwordless authentication through (Windows Hello for Business, Microsoft Authenticator, and FIDO2 security keys) or Passwords + 2-factor authentication. *Windows Hello* and the *Microsoft Authenticator* both feature either biometrics or a PIN as part of the authentication ceremony. FIDO2 keys can incorporate gestures, which Part 11 considers as biometrics. Of note, some security providers, such as Yubikey and Thales devices, are FIPS certified. Many Identity Providers support biometric authentication such as: Oracle Identity Cloud Service, Symantec Identity Security Solutions, Duo, OneLogin, Ping, Okta, and others.

§ 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.

Ignition capability: User logins are unique, ensuring that no two individuals have the same combination of identification code and password. Multi-factor authentication is recommended as an extension of the intent of this requirement.

Tip: It is up to the customer to enforce policy requiring each user to use a unique account. Shared or group accounts generally violate Part 11 record accountability requirements. Customers may have legitimate requirements for group accounts, such as driving large screen displays. Usage policy should be clear with supporting technical controls (e.g. designated computers only, no ability to change records, etc.).

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

Ignition capability: Inherited by design. Identity systems including Active Directory and Identity Providers include robust mechanisms to ensure credential validity, tied to users. The requirement can alternatively be satisfied with procedural controls.

Tip: Multi-factor authentication and "passwordless authentication" represent the current best practice. NIST Identity Guidelines (SP 800-63 series) no longer recommend arbitrary time-based password changes. Password focus is on complexity without requiring special characters and allowing secure password managers. Better yet, modern standards supersede the need for codes and passwords to be periodically checked.

(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.

Ignition capability: Inherited by design. Identity systems, including Active Directory, offer mature revocation capabilities tied to users that properly invalidate credentials. The requirement can alternatively be satisfied with procedural controls.

(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.

Ignition capability: Ignition offers numerous mechanisms to detect and prevent unauthorized usage. Typical approaches include: account lockouts, logging, and notification. Best practices are inherited by design, leveraging integrated capabilities with the external Identity Provider such as Active Directory or Microsoft AzureAD.

Customer responsibility: Internal policies and response to unauthorized use is a customer responsibility. The customer's legal and HR teams, system integrators, and consultants may be able to assist with industry best practices for dealing with unauthorized use.

(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.

Ignition capability: Inherited by design. Identity system security mechanisms occur centrally with strong cryptography. Tampering with end user devices is unlikely to help obtain unauthorized system authentication or authorization with modern systems. This is especially true with Identity Providers implementing multi-factor authentication. The requirement can alternatively be satisfied with procedural controls.

Customer responsibility: Customers have the option to test devices and tokens as part of their validation process, which can include physical verification. Identity assurance has matured since this guidance. Customers should adhere to organizational cybersecurity best practices.

Appendix A - References

References

FDA, 21 CFR Part 11, *Electronic Records; Electronic Signatures; Final Rule.* Federal Register Vol. 62, No. 54, 13429, Mar 1997.

FDA, *Withdrawal of Draft Guidance for Industry on Electronic Records; Electronic Signatures, Electronic Copies of Electronic Records*, Feb 2003.

FDA, *Part 11, Electronic Records; Electronic Signatures — Scope and Application*, Aug 2003.

FDA, *General Principles of Software Validation; Guidance for Industry and FDA Staff*. Jan 2002.

FDA, *Q7 Good Manufacturing Practice Guidance for Active Pharmaceutical Ingredients; Guidance for Industry*. Sept 2016.

FDA, *Q8, Q9, and Q10 Questions and Answers (R4)*. Nov 2011.

FDA, *Process Validation: General Principles and Practices*, Jan 2011.

FDA, *Guidance for Industry Computerized Systems Used in Clinical Investigations*, May 2007.

FDA, *Data Integrity and Compliance With CGMP Guidance for Industry*, Dec 2018.

FDA, Cybersecurity, Digital Health Center of Excellence, retrieved Aug 2022.

ISPE, *GAMP 5 A Risk-Based Approach to Compliant GxP Computerized Systems*, Second Edition. Jul, 2022.

ISPE, *Good Practice Guide: Process Validation.* Mar, 2019.

Related References

FDA Cybersecurity portal under the Digital Health Center of Excellence

FDA, Guidance for Industry. *Off-The-Shelf Software Use in Medical Devices*. Sept, 2019.

FDA, *NIST Request on Presidential Executive Order: Comments Submitted by the FDA*. May, 2021

Related Resources (Global)

PIC/S Good Practice for Computerised Systems in Regulated “GxP” Environments

2016 WHO Guidance on Good Data and Record Management Practice

2018 MHRA (Medicines & Healthcare products Regulatory Agency (MHRA)) ‘GXP’ Data Integrity Guidance and Definitions

Appendix B - Getting Started

Tip: This section provides tips on learning more about Part 11 and recommendations before starting a Part 11 project.

Review Guidance

1. Review this guide and Part 11 Guidance
2. Review 2003 revised Part 11 Guidance to Industry (Appendix A)
    a. Identify Part 11 applicability. Note the narrower standards.
    b. Additional guidance offered on: validation, audit trails, and records retention.
3. Consider purchasing the 2022 GAMP 5 Second Edition for GxP best practices.
    a. Key elements include planning, risk assessments, testing strategies.
    b. Validation reporting. Level of detail should reflect risk, complexity, and novelty of the system. Summary of: activities (verification, test report), deliverables (SOP), deviations and corrective actions, status of system and statement of fitness, and user training and knowledge management. Hardware configuration management and change control.
        i. Consider GAMP 5 Categories of software (12.3) for validation best practices. SCADA is “Category 4,” with custom scripting, queries, and programming as “Category 5.” Part 11 projects inherently require a high level of validation based on customization to meet user requirements.

First Steps

1. Understand project requirements and scope
2. Identify Stakeholders and External Requirements
    a. Determine responsibilities (e.g. Production, QA, Compliance, IT, OT, etc.)
        i. Who is the project manager? Executive sponsors?
        ii. Will system integrators or contractors be involved?
    b. What systems need to be integrated? Architecture? Desired state?
    c. Data and process owners? Stakeholders?
3. Consider external expertise
    a. Consultants, System Integrators with domain expertise
        i. IA System Integrator Program (> 2,700 SIs)
    b. Reach out to relevant PaaS platforms and specific solution providers
        i. 4IR Solutions (PharmaStack)
4. Risk Assessment
    a. Part 11 compliance risk assessment, data integrity controls and/or address risks

b. Does a privacy assessment need to be completed?
c. Assess the security practices of hardware and software vendors including integrated dependencies (e.g. Software Bill of Materials (SBOM)).

Appendix C - FDA Part 11 GFI Summary

FDA Part 11 Guidance For Industry (GFI) on Part 11

FDA Guidance For Industry contains Part 11 “Nonbinding Recommendations” and shares FDA’s “current thinking”.

- Acknowledges Part 11 concerns from industry feedback
  - (1) unnecessarily restrict the use of electronic technology in a manner that is inconsistent with FDA's stated intent in issuing the rule,
  - (2) significantly increase the costs of compliance to an extent that was not contemplated at the time the rule was drafted
  - (3) discourage innovation and technological advances without providing a significant public health benefit.
- Notes the intent to re-examine Part 11, resulting in anticipated change via rulemaking.
- Refers to collective requirements (Part 11, PHS Act, FDA regulations) as *predicate rules*.
- Recommends organizations narrow applicability of Part 11 *records* and document decisions in Standard Operating Procedures (SOPs) to electronic records used:
  - *In place of paper format*
  - *In addition to paper format* and *relied on to perform regulated activities*.
  - Submitted to the FDA under predicate rules in electronic format
- ***Validation*** is suggested to consider predicate rule requirements and system impact on: accuracy, reliability, integrity, availability, and authenticity of required records and signatures. Consider industry guidance such as GAMP standards (ISPE organization) or ISO/IEC standards.
- ***Audit Trail*** controls are suggested to be based on a justified and documented risk assessment that considers the potential effects on product quality, safety, and record integrity. Predicate rules must be met.
- ***Record Retention*** is suggested to satisfy predicate rules and be based on a justified and documented risk assessment that includes a determination of the value of records over time. The FDA does not intend to object to the use of non-electric media or choice of electronic format.

GFI References

FDA, *Withdrawal of Draft Guidance for Industry on Electronic Records; Electronic Signatures, Electronic Copies of Electronic Records*, Feb 2003.

FDA, *Part 11, Electronic Records; Electronic Signatures — Scope and Application*, Aug 2003.

FDA, *General Principles of Software Validation; Guidance for Industry and FDA Staff*. Jan 2002.

FDA, *Guidance for Industry Computerized Systems Used in Clinical Investigations*, May 2007.

FDA, *Data Integrity and Compliance With CGMP Guidance for Industry*, Dec 2018.

Appendix D - Validation and Qualification

Validation

Additional information: Validation is a frequent term used in GxP applications. It comes up in the context of software validation, which applies to software vendors and certain end user cases such as embedded firmware on medical devices. Process validation helps ensure quality, safety, and efficacy, which relates most directly to customers' holistic CGMP methodology. Per 2018 FDA CGMP Guidance to Industry, "In computer science, validation refers to ensuring that software meets its specifications. However, this may not meet the definition of process validation as found in guidance for industry Process Validation: General Principles and Practices: 'The collection and evaluation of data ... which establishes scientific evidence that a process is capable of consistently delivering quality products.'"

Software Validation

Additional information: Software validation is "confirmation by examination and provision of objective evidence that software specifications conform to user needs and intended uses, and that the particular requirements implemented through software can be consistently fulfilled." FDA, *General Principles of Software Validation; Guidance for Industry and FDA Staff*. Jan 2002. Inductive Automation provides a high level of assurance of software validation by including a separate quality assurance division throughout the entire software development lifecycle from design through release. Every code change is associated with a project management ticket that includes a "definition of done" that a developer attests to and QA engineer must independently validate prior to code inclusion. Similar software validation techniques, including formal configuration control with testing, are possible for customers at the application level under the shared responsibility model. Third-party tools such as organizational portals or systems like Kneat or Confluence & Jira (with added plugins) can help organize process validation.

Process Validation

Additional information: Process validation is defined as "the collection and evaluation of data, from the process design stage through commercial production, which establishes scientific evidence that a process is capable of consistently delivering a quality product. Process validation involves a series of activities taking place over the lifecycle of the product and process." FDA, *Process Validation: General Principles and Practices*, Jan 2011. Ignition includes tools that

can help, particularly with stage 3, “continued process verification” by tracking incoming, in-process, and finished material.

Process Validation Lifecycle

Additional information: The process validation lifecycle includes 3 stages: process design, process qualification, and ongoing process verification. (FDA, *Q8, Q9, and Q10 Questions and Answers (R4); Guidance for Industry.* Nov 2011.

Stage 1 (process design) involves capturing knowledge of the product manufacturing process and developing a process control approach.

Stage 2 (process qualification) involves the design and qualification of the building, equipment and process as well as the process performance qualification.

Stage 3 (ongoing process verification), sometimes referred to as continued process verification (CPV), involves monitoring the process, collecting and analyzing data, to demonstrate the state of control of the manufacturing process.

Tip: The Ignition platform does not inherently address the process validation lifecycle, but can be a useful supporting tool. For example, Ignition could be used to monitor and extract data regarding the facility environment, process, and utilities. Ignition is arguably best suited for stage 3 process validation, but could be used to support the entire lifecycle.

Qualification

Additional information: Qualification is the “action of proving and documenting that equipment or ancillary systems are properly installed, work correctly, and actually lead to the expected results.” “Qualification is part of validation, but the individual qualification steps alone do not constitute process validation.” FDA, *Q7 Good Manufacturing Practice Guide for Active Pharmaceutical Ingredients; Guidance for Industry.* Sept 2016.

Qualification Versus Validation

Additional information: Qualification relates to equipment, systems, or software whereas Validation refers to process. Software validation is a very specific concept.

Appendix E - Cybersecurity

Frameworks

Adopting and certifying to a standard cybersecurity framework is a best practice to demonstrate due diligence.

Standard	Summary
ISO/IEC 27001/270018	Specification for Information Security Management System; Protection of personal data in the cloud.
NIST Cybersecurity Framework (CSF)	Set of optional standards, best practices, and recommendations for improving cybersecurity and risk management at the organizational level.
AICPA SOC 2	Framework and auditing procedure to demonstrate security and privacy practices for service providers.
Other standards	Many options; Center for Internet Security (CIS); The Standard Information Gathering (SIG) Lite questionnaire

Security Controls

“Controls” refer to a process, policy, device, practice, configuration, or other action taken to modify risk. The industry best practice, as noted in GAMP 5, is performing risk-based security assessments and tailoring controls based on organization requirements. All controls should be documented and auditable.

Control Type	Meaning
Technical Controls (T)	Safeguards primarily implemented through hardware, software, physical, or environmental mechanisms.
Operational Controls (O) “procedural” or “administrative”	Primarily executed by people (as opposed to systems). Examples include documented: policies, processes, and procedures.
Inherited Controls (In) “common controls”	Security or privacy protections developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides.

Cybersecurity Information

US Government Cybersecurity Update

Inductive Automation recommends alignment with Executive Order (EO) 14028 “Improving the Nation's Cybersecurity” (May 2021) and subsequent correspondence based on National Institute for Standards and Technology (NIST) standards and Cybersecurity & Infrastructure Security Agency (CISA) guidance. Part 11 applications qualify as “EO-critical software” based on “is designed to control access to data or operational technology.” The FDA hosts a Cybersecurity portal under their Digital Health Center of Excellence which references CISA guidance and NIST standards, including acknowledging the call for position papers responding to EO 14028 (FDA, 2021). As of 2022, the FDA focus is on medical device manufacturers (MDMs) and health care delivery organizations (HDOs), but current cybersecurity guidance is broadly applicable to all Part 11 applications.

Tip: Consider CISA Shields Up and Multi-factor Authentication (MFA) guidance. NIST also provides useful recommendations: Cybersecurity Insights Blog, Assessment & Auditing, MFA, Identity and Access Management, and Cybersecurity Frameworks.

Identity and Access Management

Identity and Access Management (IAM) is a cornerstone of achieving high levels of assurance with data integrity and ALCOA+. IAM systems are often referred to as “Identity Providers” or IdPs. Simply put, there is little value in auditing if records cannot be trusted. Electronic systems depend on *Authentication*, which verifies identity or an assertion, and *Authorization*, which determines access rights.

Modern approaches to IAM can be deployed on premise or in the cloud. Cloud offerings tend to be more capable. Example characteristic features:

- Multi-factor authentication (MFA) for users; passwordless; certificates for systems.
- User-based provisioning. Stakeholders, not Sysadmins, can manage groups
- Entitlement management. Users grant access to applications or platforms
- Privileged identity management. Time-restricted or workflow-based privileged roles
- Single sign-on (SSO) and federation
- Policy engines; pattern of use; location or time; device health checks

Inductive Automation recommends the use of modern IAM systems tailored to meet business requirements informed by risk assessments. Selecting an appropriate IAM foundation strongly supports applicable Part 11 requirements. Cloud examples include: Microsoft Azure AD, Oracle Identity and Access Management Products (multiple), IBM Security Verify Access, Duo, Okta IAM,

and RSA SecurID. On premise examples include: HashiCorp Vault, Apache Keycloak, and Red Hat Identity Management.

Additional information: Ignition is designed to interoperate with identity providers using the SAML or OpenID Connect protocols. Authorization works by mapping IdP groups or roles to Ignition Security Levels. This extends the benefits to Ignition including: policy engines, governance, multiple factors, device support, management, auditing, federation, integration, etc. Generally speaking, modern IdPs tend to provide the strongest and most flexible options.

For many applications, the next best IAM approach integrates with Enterprise systems, often maintained by IT or OT departments. A common industry example is with Active Directory integration using Microsoft Windows Domains or other systems using combinations of longstanding protocols such as: LDAP, RADIUS, and Kerberos. A variety of legacy and modern products define this space. Customers are encouraged to align with organizational policy.

Security Resources

Inductive Automation Security Portal, Ignition Security Hardening Guide and FDA Cybersecurity portal under their Digital Health Center of Excellence
CISA Shields up, ICAM resources, and Multi-factor Authentication (MFA) guidance.
NIST recommendations: Cybersecurity Insights Blog, Assessment & Auditing, MFA, Identity and Access Management, Digital Identity Guidelines (800-63 series), and Cybersecurity Frameworks.

Cloud Part 11 Resources

Amazon AWS 21 CFR 11 Best Practices, Config Doc. AWS Well-Architected Framework.
Microsoft Azure 21CFR11 portal, Azure GxP Guidelines (includes Part 11 & European standards). Azure Well-Architected Framework.
Google provides GxP and 21 CFR Part 11 guidance

Appendix F - Inductive Automation Software Development Practices

Ignition DevSecOps SDLC

The Inductive Automation (IA) Software Development Lifecycle (SDLC) is generally aligned with GAMP 5 recommendations. It is a coordinated effort based around: people, processes, and technology that covers a single common code base. Ignition is divided into “Product Areas” under the responsibility of Product Owners (POs). Cross-functional teams of 5-9 members including QA and design group work based on a ticket system within a larger project management suite. Ignition is released on a five week “release train” based on week-long integrated Development, Security, and Operations (DevSecOps) “sprints” following accepted agile development methodologies. Nightly builds are automatically generated and made available on the IA website for all modules, operating systems, and platforms. All stakeholders including senior developers and QA engineers attest that all required steps were properly completed on digital “release checklists” for scheduled and out of band releases.

Inductive Automation (IA) is 95% complete with self-certification of NIST Guidelines on Minimum Standards for Developer Verification of Software (July 2021), written in support of the 12 May 2021 Executive Order (EO)14028 on Improving the Nation’s Cybersecurity. Inductive Automation is actively pursuing ISA/IEC 62443 certification on Software Development Lifecycle Assurance to formalize development practices, having completed a gap analysis with the certification body in Q2 2022. Inductive Automation keeps up with current recommendations from NIST and the Cybersecurity and Infrastructure Security Agency (CISA) and helps customers achieve standards with Ignition.

IA utilizes an independent QA department with a target of a 1-to-1 parity between Software Engineers and QA Engineers. QA is involved in all stages of the SDLC from planning, design, implementation, testing, and ongoing support and has representation on all development teams. QA conducts a range of manual and automated testing modalities in support of stability, security, performance, and quality, across the spectrum of Ignition functionality.

Ignition, including all modules and target architectures, is only ever built on a single Continuous Integration, Continuous Delivery (CI/CD) pipeline that exists in a physically protected, monitored, dedicated environment. The practice eliminates build variance from developer environment configuration. A CI tool regularly performs static code analysis, inspecting code branches to detect bugs and security vulnerabilities, as well as measuring the technical quality in terms of potential defects, vulnerabilities and maintenance risk. A separate tool provides composition analysis, focusing on third-party libraries through continuous vulnerability scans and assessments

for: security, license, and operational risks of dependencies. The tool generates a “Software Bill of Materials” that is bundled with each release. “Red” vulnerabilities are remediated prior to release, controlled by “release checklist” and the project management system.

Technical controls enforce strict adherence to a standard “Git Fork & PR workflow”, ensuring that no direct changes are ever made to the main repository and forming a core part of the quality process. Every single code change must be reviewed and is subject to significant checks. Each pull request (PR), which is a potential software change referencing one or more tickets, triggers a review and testing process. The CI/CD pipeline creates a full Ignition build with the potential change. The build ensures that the change properly compiles, passes strict automatic code-style guidelines (checkstyle), and that all unit and module tests pass. Reliable human review with 2-person integrity requires a senior developer to digitally sign off on a code review for each PR. Developers have access to individual repository accounts, but do not have access to code signing certificates, which are managed centrally by trusted agents. If the build succeeds, the CD system orchestrates a Docker container running Ignition on the candidate build for testing purposes. Automatic validation testing starts with automatic integration testing through multiple tools and frameworks on the candidate “build.”

QA performs verification testing based on "Definition of Done" as a step for each ticket in the project management platform. QA also performs numerous validation and other tests including: load/stress testing, functional, integration, regression, and operational testing in dedicated environments with a variety of tools. The QA test plan includes manual testing and testing outside the release cycle.

Appendix G - Case Studies and Reference

Environmental Monitoring System in Pharmaceutical Industry for Meeting FDA GMP Compliance. Neomatrix. A leading regenerative medicine company created a GMP and 21 CFR Part 11-compliant application using Ignition software and Rockwell ControlLogix hardware utilizing the PlantPAx architecture.

Improved Data Integrity and Easier Compliance with 21 CFR Part 11. Grantek. Par Pharmaceutical Part 11 compliant project.

Variety of Connections, Unlimited Licensing Aid Cancer Therapy New SCADA Delivers Compliance, Mobility, Lower Costs, and More. Autolus Therapeutics. Autolus is a London-based biopharmaceutical company that delivers T cell therapies to cancer patients. The application satisfies Part 11 and the European Union equivalent, EudraLex Annex 11.

Ignition SCADA Improvements for Pharmaceutical Manufacturer. Tiga. A leading pharmaceutical manufacturer achieved FDA regulation 21 CFR Part 11 compliance with Ignition.

Helping Customers with 21 CFR Part 11 Software Provides FDA Compliance for Pharma, Along with Speed and Flexibility. Snapdragon. Snapdragon Chemistry adopted an Ignition SCADA system to achieve 21 CFR Part 11 compliance.

Pharma Company Meets Standards for 21 CFR 11 with Ignition Success Inspires Plans for Expansion. Bachem. A Swiss-based biochemical company uses Ignition to achieve Part 11 compliance.

21 CFR Part 11 Compliance with Inductive Automation's Ignition Platform. Panacea. Ignition configuration tips and best practices to achieve Part 11 compliance.

Authors

This guide is the result of a collaborative effort between Inductive Automation and industry leaders in the Pharmaceutical and Food & Beverage industries. Individual authors and their companies are outlined below.

Inductive Automation:
Inductive Automation creates industrial software that empowers customers to swiftly turn great ideas into reality by removing all technological and economic obstacles. The software platform, Ignition by Inductive Automation, is the world's first database-centric, web-deployed, 100% cross-platform, unified HMI, SCADA, IIoT, and MES solution. Ignition is used across the globe in over 100 countries and in virtually every industry.

Inductive Automation website: https://inductiveautomation.com/

Nathan Boeger:
Nathan Boeger is responsible for furthering internal compliance and helping customers succeed at Inductive Automation (IA). He recently retired as a United States Navy Information Warfare Officer after 20 years of service. He is a new ISPE member and FDA compliance enthusiast. Nathan holds an MS in Cybersecurity from Carnegie Mellon University, a BA in Computer Science from UC Davis, and numerous technical certifications including CISSP-ISSAP from ISC2.

Follow Nathan on LinkedIn: https://www.linkedin.com/in/nathan-boeger/

Madison Knowles:
Madison Knowles leads the Operations group within Sales Engineering at Inductive Automation. She has held numerous roles within IA including project and program management. Madison holds dual degrees from the University of Arizona, a BS degree in Physical and Biological Anthropology, and a Bachelor of Fine Arts in Dance. She holds an AA degree in interdisciplinary studies in math and science.

Follow Madison on LinkedIn: https://www.linkedin.com/in/madison-gelien-knowles

4IR Solutions:
4IR Solutions provides a fully managed hybrid cloud infrastructure that enables life sciences and other manufacturers to simplify their operational technology, increase efficiency and scalability, and reduce needed resources and costs. Featuring best-in-class secure IT technologies, stable

plant floor applications, and seamless automation that creates a simple experience for both end users and service providers.

4IR Solutions, manufacturing cloud infrastructure, simplified. Because efficient solutions shouldn't be complicated.

4IR Solutions Website: https://www.4ir.cloud/

> **Joseph Dolivo:**
> For more than a decade, Joseph has focused on modernizing manufacturing by intelligently adopting state-of-the-art technologies and principles from the software industry. Joseph is passionate about inspiring his team and customers with his experienced industry knowledge and deep diving on all things technology. Having worked in a variety of key consulting and decision-making roles, Joseph currently serves as the CTO of 4IR Solutions, turning "the Cloud" and "DevOps" into practical realities for life sciences and other manufacturers today.
>
> Follow Joseph on LinkedIn: https://www.linkedin.com/in/josephdolivo/

Grantek:
For over 40 years, top manufacturers in Food & Beverage, CPG and Life Sciences/Pharmaceuticals have called upon Grantek to solve their most complex business and manufacturing challenges. Grantek automates Pharmaceutical and Food & Beverage manufacturing operations, including integration with business systems for seamless solutions. Grantek helps customers meet the stringent requirements and challenges of the 4th Industrial Revolution. Grantek is a system integrator and solution provider with a specialization in Smart Manufacturing solutions, Manufacturing Automation solutions, Industrial IT/Cybersecurity solutions and Manufacturing Consulting services.

> **Bryon Hayes:**
> Bryon Hayes, P.Eng. is the Director of Smart Manufacturing Solutions at Grantek Systems Integration Inc., where he manages a portfolio of products and solutions aimed at supporting the life sciences manufacturing industry. He has over twenty years' experience executing and managing automation and information projects for pharmaceutical manufacturers. Bryon is heavily involved in the life sciences industry, being an active member of ISPE since 2009, and a member of both the Pharma 4.0 Special Interest Group and the Blockchain Special Interest Group. Bryon holds a Bachelor of Applied Science degree in Systems Design Engineering from the University of Waterloo in Waterloo, Ontario, Canada.

Wunderlich-Malec Engineering:
Clients in a wide variety of industries across the globe rely on Wunderlich-Malec for advanced engineering solutions. Many of them are looking to improve profitability or expand their business operations, and since 1981 Wunderlich-Malec has excelled at creating and deploying the total solutions they need to meet their business objectives. We believe the key to our success is our depth of talent, proven methodologies, and exceptional flexibility. As a 100% Employee-Owned Company our people are passionate about solving your unique engineering challenges, and with the support of industry experts behind them, they can successfully execute projects of any size while meeting your requirements of scope, schedule, and budget.

Kelvin Yeow:
Kelvin Yeow, PMP. is the Business Unit Manager at Wunderlich-Malec Engineering, Inc., where he leads the life science focused system integration team based in Boston, MA. He has over twenty years' experience delivering GMP Batch and Automation solutions in the life science industry. Kelvin holds the degree of Bachelor of Science in Electrical Engineering from the Illinois Institute of Technology.

Fred Zaboli:
Fred Zaboli is the Engineering manager in Wunderlich-Malec's Orange County, CA office, He brings over Twenty-plus years of engineering leadership working in a variety of vertical markets such as Pharmaceutical, Food, and Beverage (Brewing) Power, Oil & Gas, and Water & Wastewater industries. He is experienced with all phases of a project, including planning, cost estimation, scope definition, scheduling, technical lead, detailed design, programming, field commissioning, startup, and operations. Fred has a Bachelor of Science degree in Electrical Engineering from the University of Technology, Tehran.