VAISALA

Application Note

www.vaisala.com

21 CFR Part 11 compliance for environmental monitoring software functions Vs. operating procedures

Regulatory changes come in waves. Over the last 20 years, there have been a few virtual tidal waves involving the use of computerized systems in GxP-regulated applications. The first centered on the FDA's Title 21 CFR Part 11 in 1997.

The next big wave of regulatory change was in the principles of Good Distribution Practice. Major standards include:

- United States Pharmacopeia (USP)
  - USP General Chapter <1079> Good Storage and Shipping Practices
  - USP General Chapter <1083> Good Distribution Practices—Supply Chain Integrity
- European Medicines Agency (EMA)
  - Guidelines on Good Distribution Practice of Medicinal Products for Human Use
  - Directive 92/25/EEC
- World Health Organization (WHO)
  - Good Distribution Practices for pharmaceutical products TRS No. 957, Annex 5 (2010)
  - Model requirements for the storage and transport of time and temperature sensitive pharmaceutical products TRS No. 961, Annex 9 (2011)

The next great wave of changes to regulations came with a focus on data integrity. This has seen the publication of numerous guidance documents, including:

- The Food and Drug Administration (FDA) Draft Guidance: "Data Integrity and Compliance With CGMP Guidance for Industry"
- Medicines and Healthcare products Regulatory Agency (MHRA) – "Guidance on GxP Data Integrity"
- Pharmaceutical Inspection Co-operation Scheme (PIC/S) Draft Guidance "Good Practices for Data Management and Integrity for Data Management and Integrity in Regulated GMP/GDP Environments"
- World Health Organization Draft Guidance: "Guideline on Data Integrity"

The next wave: From validation to assurance

The latest shift in regulatory focus on electronic records is the switch from CSV (Computer Systems Verification) to CSA (Computer Systems Assurance). These changes and their regulatory guidance (such as Part 11), were meant to help firms cope with the emergence of cloud computing that has allowed the use networked remote servers hosted on the Internet to process, manage, and store data. This latest change has exposed the risks inherent to computerized systems with documentation strategies that were designed for mechanical equipment.

While these changes in the regulatory world appeared as separate events, they are connected. All were based on the intersection between existing GxP concerns and changing technology. 21 CFR Part 11 mitigated the risks of moving from paper to electronic records. Changes to Good Distribution Practice GDP allocated equal responsibility to everyone associated with a product—from handling raw materials to distribution of finished products. Guidance on data integrity asks us to think holistically about recording, communicating, and storing data. Computer Systems Assurance focuses on testing software and systems to ensure product efficacy and safety. Thus in 2020, the Food and Drug Administration announced the publication of a new draft guidance: "Computer Software Assurance for Manufacturing, Operations, and Quality System Software".

Connecting the dots

Over the years, GxP-regulated industries have responded to each wave of regulatory changes separately. Individual companies—often responding to enforcement action—tried to patch potential holes in their systems with targeted audits. In audits, there has been an increasing focus on electronic records and electronic signatures (ERES), system validation, and data integrity.

However, too often an audit process can cause a focus on compliance for compliance's sake.

It helps to remember that 21 CFR Part 11 did not come into existence to create compliance with its guidelines. The purpose was to connect written or electronic signatures to their records and ensure that documents and signatures created electronically were authentic. This is an important distinction.

Even so, soon after its publication companies began asking vendors if their systems were compliant with Part 11. However, 21 CFR Part 11 does not apply to system vendors. The regulation applies to the regulated application and the firm responsible for it. Further, the actual compliance part of a system lies in how it is used. A better question to a system vendor would be: "If we use your system, will we be able to operate it in a manner that is compliant with 21 CFR Part 11?"

Revisiting 21 CFR Part 11

Our path to understanding how to comply with 21 CFR Part 11 must begin with the regulation itself. It is barely more than two pages and split into three subparts.

- Subpart A "General Provisions"
- Subpart B "Electronic Records" with 4 sections
  - Section 11.10: Controls for Closed Systems
  - Section 11.30: Controls for Open Systems
  - Section 11.50: Signature Manifestations
  - Section 11.70: Signature Record Linking
- Subpart C "Electronic Signatures"

In environmental monitoring systems like Vaisala's viewLinc Continuous Monitoring System (CMS), Subpart A is not highly relevant, except for three definitions:

- Closed system: An environment in which system access is controlled by persons who are responsible for the content of electronic records within the system.
- Electronic record: 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 system.
- Electronic signature: A compilation of data that includes any symbol, or series of symbols, that are executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.*

These definitions allow us to clarify how 21 CFR Part 11 applies to environmental monitoring systems used in a GxP-regulated application:

- The data in the system are classified as electronic records.
- Subpart B Section 11.10 applies because monitoring systems are closed systems.
- Section 11.30 does not apply to a monitoring system because it pertains to open systems.
- Subpart C, and the rest of Subpart B (11.50 and 11.70), may not apply because monitoring systems do not typically use electronic signatures for review of data.

The section of Part 11 that is directly related to a continuous monitoring system is Section 11.10 "Controls for Closed Systems".

> *"Persons who use closed systems for electronic records shall use procedures and controls to protect the authenticity, integrity, and confidentiality of the records, and to ensure that signed records can't be repudiated."*
>
> From 11.10: Controls for closed systems

In a monitoring system, "procedures and controls" refer to the methods we use to protect the authenticity, integrity, and confidentiality of the records.

Procedures and controls, in order of importance, come from three sources:

- Actions performed by a system user.
- Functions built into the software.
- Services provided by the vendor.

Note that procedures and controls performed by a system user comprise *most* of the compliance activities for Part 11.

**21CFR11 Subchapter A - General, Part 11, Electronic records; electronic signatures, Sec. 11.3 Definitions*
www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm

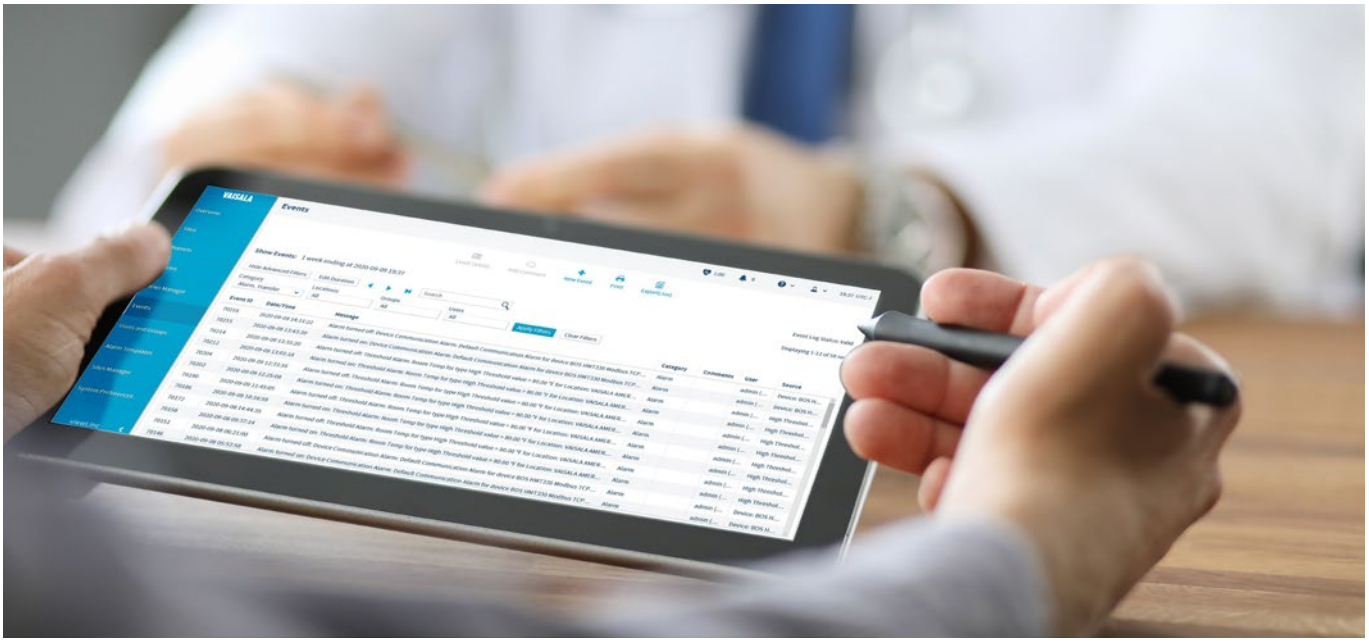
The closed system procedures and controls for Part 11 are as follows:

- Validation
- Generate accurate and complete copies in human-readable form and electronic form
- Protection of records to ensure accurate and easy retrieval throughout the records retention period
- Limited system access to authorized individuals
- Audit trail
- Operational system checks to enforce sequencing of events and steps
- Authority checks to ensure only authorized individuals can use the system or perform the operation at hand
- Device checks to determine the validity of data input
- Training
- Written policies to hold users accountable for actions taken and records created electronically
- Controls over system documentation, including:
  - System operation and maintenance documentation
  - Revision and change control procedures for developing and modifying system documentation

In the table below we see how each procedure and control method is performed; by system software, system users, or both. Capitalization represents where functional responsibility is *primary* and sentence case represents where responsibility is secondary.

Item	User Procedures	Software Function	Vendor Service
Validation	YES		yes
Complete Copies		YES	
Record Protection	YES	yes	
Limit System Access	YES		
Audit Trail	yes	YES	
Operational Checks	yes	YES	
Authority Checks	yes	YES	
Device Checks		YES	
Training	YES		yes
Written Policies	YES		
System Doc Controls	YES		

We can review each item and further define where compliance with 21 CFR Part 11 depends upon user actions, software functions, or a combination.



Procedures & controls

Validation:

Validation is a costly element of compliance. It can only be effective if the user has procedures in place to guide the validation effort. Thus, validation procedures are an expectation in GxP-regulated industries. Many environmental monitoring systems have options to simplify validation. For example, the viewLinc system has a standard Installation Qualification/Operational Qualification (IQOQ) document. In some regions, Vaisala can provide validation execution as a service. System vendor validation services can save in-house resources.

Generate accurate and complete copies in human-readable form and electronic form:

This requirement is one of two that can only be fulfilled by a system's software. A monitoring system must generate complete human-readable copies of electronic records. Fortunately, this requirement is also one of the core functions of any monitoring system designed to function in a GxP-compliant application.

Protection of records to ensure accurate and easy retrieval throughout records retention period:

Record protection is primarily reliant on procedures executed by a system user or their IT team. While it is necessary to protect data from deletion from inside the application, long-term data protection is really a function of IT procedures that follow best practices for data backup, storage, and archiving.

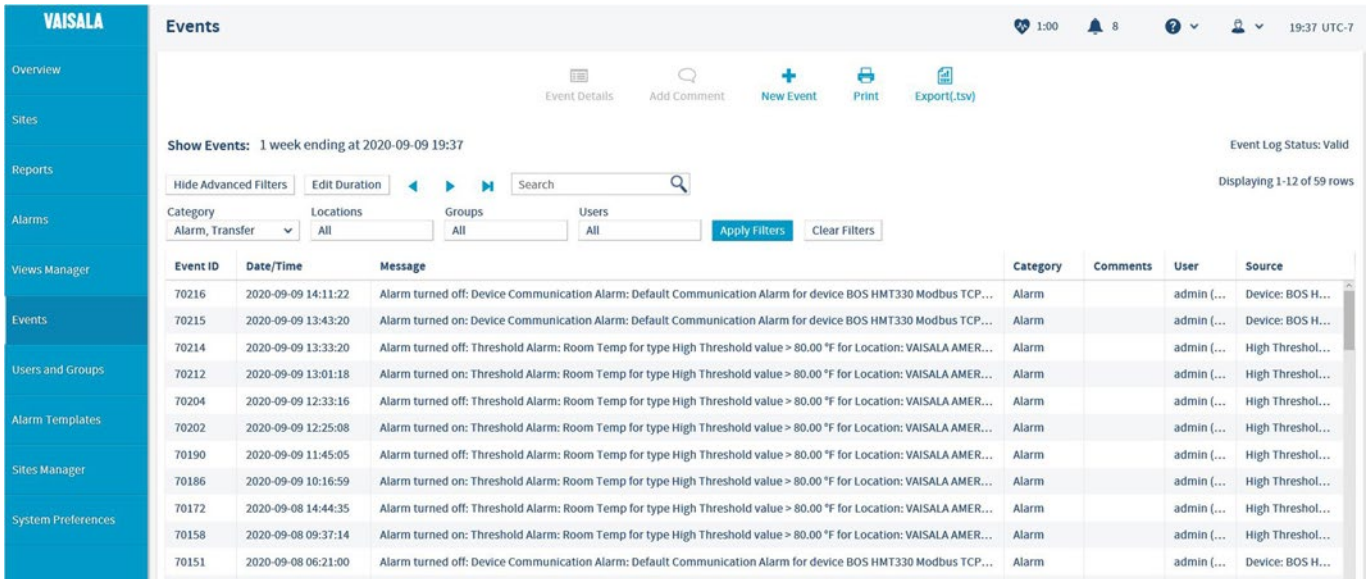
The Vaisala viewLinc system was designed to simplify data protection and accessibility of records. The software achieves this in two ways: by making data records very small, and by ensuring that software versions are always backwards compatible. Small record size in viewLinc means data can be stored in the database for easy retrieval, instead of being exported to an archive. Backwards compatibility ensures that viewLinc records can always be accessed on any future version of the software.

Limit system access to authorized individuals:

This requirement is fulfilled by a user procedure. Procedures must be in place to limit access to the system and the facility being monitored. This is especially important with a monitoring system, where data is collected by data loggers that are dispersed across a facility in areas of varying security. Limiting physical access to authorized persons is a norm in almost every GxP facility, so fulfilling this requirement rarely takes extra effort.

Audit trails:

The audit trail is a vital Part 11 requirement that can only be fulfilled by a software function. The monitoring system must have this function to track all events that create, alter, modify, or delete records in the system. However, audit trails are insufficient without regular review. It does not matter if the audit trail records data alterations if no one is reviewing the audit trail to see that the data was altered.



Operational system checks to enforce sequencing of events and steps:

This control is important for systems that have complicated workflows. In a typical monitoring system like viewLinc, the workflow is quite simple and varies little from application to application. The viewLinc software includes workflows as a software function so that users can simply model their procedure after the pre-existing workflow. This make sense because some companies do not consider monitoring procedures to be a place of strategic competence where customizing the workflow would provide a competitive advantage.

Ideally, a monitoring system should not require any customization and a standardized system saves on validation time. However, this should not impart a false sense of security. In the viewLinc system, workflow steps are enforced. However, monitoring system administrators still need Standard Operating Procedures (SOP) to guide users.

Authority checks to ensure only authorized individuals can use the system, or perform the operation at hand:

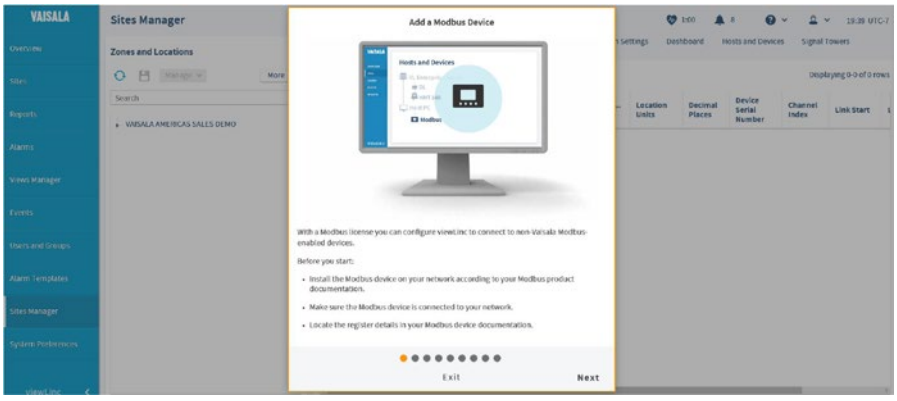
Typically, authority checks are enforced through usernames and passwords that grant system access with user profiles that define access rights within the system. Authority checks are dependent upon security features built into the system as software functions. However, actually fulfilling this requirement is dependent on a user procedure to define user roles so that access rights can be correctly assigned. Users will also need a general security policy to define expectations of password complexity, password aging, and other security parameters.

Device checks to determine validity of data input:

Device checks are the second of the two requirements that can only be fulfilled by a software function. In the viewLinc software, a device may only send data to the system if it is using the correct protocol and has been previously identified as a legitimate device by a viewLinc system administrator. Since this function is usually internal to a monitoring system, there should be no need here for a user procedure.

Training:

This is a requirement that can only be fulfilled by a user procedure. The procedure should verify that system users are trained to use the system. Often, system vendors will offer training services, as does Vaisala as part of viewLinc's support plan: The Life Cycle Maintenance Agreement. However, software can help with training. The viewLinc software has embedded screen prompts called "Tours". Tours provide guidance on common tasks; by going through the tour, the user performs the desired task.



Written policies to hold users accountable for actions taken and records made in electronic systems:

A user policy or procedure will fulfill this requirement. However, software that is designed for a regulated environment can help. For example, the viewLinc software ensures that users cannot accidentally delete a record or modify raw data. In addition, all user actions are captured in viewLinc's event log. In case of a problem, viewLinc provides a record of all actions taken.

Controls over system documentation:

A monitoring system should come with a comprehensive User Guide and online help. But this is only a small part of system documentation. This requirement also includes the records and documents that are generated during system implementation and maintenance, such as validation documentation and SOPs. These documents are typically controlled by user procedures for protected storage, change control, and revision control. This is usually done in conjunction with the documentation function of a firm's Quality Assurance department.

Compliance: A shared goal, not a shared responsibility

Compliance with 21 CFR Part 11 and other regulations is a joint effort between a system *and* its users. Users should be familiar with the regulation, which is brief, but can be difficult to analyze in terms of how much applies to in-house procedures and how much applies to software functions.

However, the fundamental responsibility for compliance with regulatory guidance lies predominantly with user procedures that define how a system is deployed, used, and maintained. This is the foundation for the compliance of all GxP systems.

It is important that any system used in a GxP-regulated application be designed for compliance activities. Many systems contain the expected features, but these can never satisfy 21 CFR Part 11 on their own.

The viewLinc software was designed to help organizations achieve compliance by simplifying procedures. Designed to operate in GxP-regulated environments, the Vaisala viewLinc Continuous Monitoring System includes: comprehensive validation protocols, multiple layers of security, and fail-safe audit trail capabilities.

VAISALA

Please contact us at
www.vaisala.com/contactus

www.vaisala.com

Scan the code for more information

Ref. B212174EN-A