XRF SYSTEMS

White paper

Supporting the pharmaceutical industry with 21 CFR Part 11 compliance readiness

Table of contents

Edition notice

Second Edition, July 2017

Acknowledgements

All trademarks ™ and copyrights © are the property of their respective owners.

Disclaimer

PANalytical B.V. makes no warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Further, PANalytical B.V. reserves the right to revise or change this document without the obligation to notify any person or organization of such revision or change. The content of this document is checked on a regular basis and subsequent editions are issued when necessary.

Introduction

The purpose of this document is to describe how PANalytical systems support system owners meeting the requirements of the 21 CFR Part 11 regulations issued by the United States' FDA.

Design and development of PANalytical systems is done according to ISO9001 and ISO14001 certified processes and procedures. These formalized processes and procedures include standards for all aspects of the development process, used in each project and safeguarded by PANalytical's quality control organization.

Integration of PANalytical systems in a 21 CFR Part 11 compliant laboratory environment is straightforward because PANalytical offers tools and services to guarantee authenticity, integrity and confidentiality of electronic records and electronic signatures. Also the final system qualification is supported with products and services.

Complete traceability and reproducibility is possible in terms of experiment, operation (automatic audit trail generation) and analysis (complete history with all parameters used to achieve the analytical results).

The proper set-up of the operating system Microsoft (MS) Windows and network tools provide security while the audit trail software detects if electronic records are made invalid or changed, guaranteeing tamperproof data.

PANalytical also offers system validation support, comprising products for installation qualification (IQ) and operation qualification (OQ), and support for design qualification (DQ) and performance qualification (PQ).

PANalytical systems

This document is applicable to the following software herein to be referred to as PANalytical software platforms:

- SuperQ
- Epsilon range

All PANalytical systems are closed systems according to FDA's definition and are subject to the controls as defined by the FDA.

A closed system is (21 CFR Part 11 Section 11.3) "an environment in which the system access is controlled by persons who are responsible for the content of electronic records that are on the system".

About controls for closed systems (21 CFR Part 11 Section 11.10): "Persons who use closed systems to create, modify, maintain or transmit electronic records shall employ procedures and controls designed to ensure 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".

System security

The PANalytical systems support networked environments, so from a single PC system to a multiple PC system in a LAN.
The access security is a two-stage process, since the user first logs on to the PC and next to the application software of the system.

The following security events are saved into the Enhanced Data Security (EDS) software module login/logoff, start/stop instrument sessions and security alarm events.
PANalytical uses the MS Windows user name and passwords. Password length, expiration period, etc. are subject to the role of the user.

Compliance with 21 CFR Part 11 makes the system owner responsible for a number of duties, these are: proper operating system configuration, putting backup and disaster recovery procedures in place and setting up and maintain a Standard Operating Procedure (SOP). PANalytical gladly offers support to help you do this.

Audit trail and traceability

Experiment traceability is a very important requirement for a proper analysis process. To guarantee this each experimental parameter regarding the sample, the instrument and its settings must be saved with the measured data. Analytical traceability goes one step further and each analysis parameter must be saved additionally. Process traceability gives the complete picture and additionally should be saved who did what, when and why.
PANalytical XRF software platforms satisfy all the above criteria.

The audit trail records contain data about process, security and electronic record traceability.
The following events are saved in the system log database: application login/logoff, unauthorized attempts handling, start/stop instrument sessions, and new/changed electronic records.
The Enhanced Data Security (EDS) system log database contains the following data, if applicable: event type, user ID, full (printed) user name, date/time (including UTC offset), electronic record identification, additional data such as sample name and sample ID.
The EDS audit trail software is always active and cannot be bypassed.
The reporting functionality of the EDS software ensures reliable copying and readability by the FDA.

Electronic records

The FDA defines in 21 CFR Part 11 electronic records as: *“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”*.

In PANalytical XRF systems electronic records comprise measurement data and analysis data. All of the records are stored in a database.

Reports can be stored in PDF file format. In addition LIMS-optimized human-readable data formats can be automatically forwarded for safeguarding and processing.
The readability of all electronic records and report files by public domain software or by the analytical software is guaranteed throughout the minimum required retention period as valid for the subject electronic records.

The electronic records contain the complete history including all parameters, for repeatability and traceability purposes.
The database that contains all electronic records can be protected from both modification and deletion using the MS Windows file security mechanisms.
Backing up and archiving can be done with any common tool made for this functionality.

Electronic signatures

PANalytical has implemented non biometric signatures. Both user name and full (printed) user name are included, as well as the date and time (including UTC offset) and the meaning of the signature (for example: data measured, approved). The identity of the signer is checked at each signing. Each signing is stored in the EDS system log database. All sessions are treated as continuous sessions on the condition that the PC is not idle for a pre-defined period of time. This means that only the password has to be given, while the system assumes that the same user is operating it.

Requirements checklist

The table below lists the specific sections and requirements of the 21 CFR Part 11 Rule. For each FDA requirement it is explained how this requirement is implemented in PANalytical XRF systems.

SuperQ and Epsilon software

Section	Requirement	PANalytical implementation
Subpart B – electronic records		
§B11.10	**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 designer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:	
(a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	• In the factory an acceptance test is executed on system level. The test is repeatable and the results are available. • Application development is validated by default by the customer and is to be arranged by means of a SOP. • PANalytical is ISO 9001 certified. • The records are stored in databases that cannot be altered outside the software system. • Extended tests are defined to validate that printed copies of electronic records and exported electronic copies of electronic records preserve the content and meaning of the record. • IQ and OQ procedures for the system are available.
(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.	• Printed copies and exported electronic copies can be generated. • Data can be exported to a LIMS. • Extended tests are defined to validate that printed copies of electronic records and exported electronic copies of electronic records preserve the content and meaning of the record.

Section	Requirement	PANalytical implementation
Subpart B – electronic records		
(c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	• The records are stored in databases that cannot be altered outside the software system. • **SuperQ**: Each time a result is recalculated or edited, the outcome of this action generates a new result with a unique version number and link to the parent result. • **Epsilon**: It is not possible to recalculate or edit results. • Records are always retrievable using the version of the software application software used to create them or newer versions. • Extended tests are defined to validate that printed copies of electronic records and exported electronic copies of electronic records preserve the content and meaning of the record. • Extended tests are defined to validate that updated records from low version numbers to high version numbers preserve the content and meaning of the record.
(d)	Limiting system access to authorized individuals.	• The software uses a user login mechanism. • The software uses a user level mechanism with which authorization can be configured for specific actions. • User identification/password validation is performed by the operating system. • Only users that are validated by the operating system can be added to the software user database as authorized users.
(e)	Use of secure, computer-generated, time stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	• The system is capable of recording all electronic record create, update, and delete operations (recorded information is event, operator-id, time, date). The audit trail system is securely retained throughout the applicable retention period. The record system is exportable to a widely used format and into human readable form (regardless the upgrades of the software or the operating system).
(f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	• The sequence of events for a measurement is fully determined by the software.

Section	Requirement	PANalytical implementation
Subpart B – electronic records		
(g)	Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation computer system input or output device, alter a record, or perform the operation at hand.	• The software uses a user login mechanism. • The software uses a user level mechanism with which authorization can be configured for specific actions. • User identification/password validation is performed by the operating system. • Only users that are validated by the operating system can be added to the software user database as authorized users.
(h)	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	• Each spectrometer is physically connected to only one computer.
(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.	• PANalytical personnel are trained according to its quality procedures. • PANalytical is ISO9001 certified and product development is done following these guidelines. All persons operating PANalytical systems should have the necessary levels of education, training, and experience to perform their assigned tasks. It is the responsibility of the system owner to ensure this. PANalytical offers a number of training courses for end-users as well as system owner's service personnel.
(j)	The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signature, in order to deter record and signature falsification	• Responsibility of system owner
(k)	Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	• All necessary documentation is included with each system delivery. PANalytical also offers system checks as part of its IQ procedure. (1) Internal distribution, access, and use of documentation is the responsibility of the system owner. (2) This is the responsibility of the system owner. PANalytical supplies all software and firmware products, as well as printed documentation with version information. If the system owner has a documentation control system this version information can be transferred to it.

Section	Requirement	PANalytical implementation
Subpart B – electronic records		
§B11.30	**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 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.	• The software is meant for closed systems.
§B11.50	**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.	• The information is stored within the electronic record or in logically associated records. • Time is stored in universal time format. • The name of signer that is to be used in reports is obtained from the operating system.
(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 from of the electronic record (such as electronic display or printout).	• The information is present on all printed and electronic reports
§B11.70	**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.	• The information is stored within the electronic record

Section	Requirement	PANalytical implementation
Subpart C – Electronic signatures		
§C11.100	General requirements	
(a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else. Are electronic signatures unique to an individual?	• Electronic signatures are always based on the unique combination of user name and password. User names cannot be re-used, re-assigned or deleted. The system owner is responsible for proper set-up in the operating system.
(b)	Before an organization establishes assigns, certifies, or otherwise sanctions an individual's signature, or any element of such electronic signature, the organization shall verify the identity of the individual.	• Not applicable. At the moment an electronic identity is issued the system owner must check the identity of the individual involved.
(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.	• Responsibility of system owner
§C11.200	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. (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 (2) Be used only by their genuine owners; and (3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.	• The software includes an encompassing set of trigger moments which require a signing action
(b)	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	• Not applicable for PANalytical

Section	Requirement	PANalytical implementation
Subpart C – Electronic signatures		
§C11.300	Controls for identification codes / passwords	
	Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:	
(a)	Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.	• This must be set-up accordingly in the operating system. The set-up and maintenance is the responsibility of the system owner.
(b)	Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	• This must be set-up accordingly in the operating system. The set-up and maintenance is the responsibility of the system owner.
(c)	Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information and to issue temporary or permanent replacements using suitable, rigorous controls.	• In PANalytical systems the operating system functionality controls user accounts and can be used to define new passwords.
(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.	• The number of unsuccessful login attempts to a PANalytical software user account or signing attempts is limited to three. The system owner is responsible for setting up these alarm destinations. All successful login and signing attempts and all alarms are stored in the audit trail.
(e)	Initial and periodic testing, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.	• Not applicable. Cards or tokens are not used.

Abbreviations

Abbreviation	Meaning
CFR	Code of Federal Regulation
CSV	Comma separated values
DQ	Design Qualification
FDA	Food & Drug Administration
G*P	Good Laboratory/Manufacturing/Automated Manufacturing/etc. Practice
IQ	Installation Qualification
ISO	International Organization for Standardization
LAN	Local Area Network
MS	Microsoft
PC	Personal Computer
PDF	Portable Document Format
PQ	Performance Qualification
OECD	Organization for Economic Co-operation and Development
OQ	Operation Qualification
SOP	Standard Operating Procedure
UTC	Universal Coordinated Time

Glossary

Terminology	Meaning
Audit Trail System	System that keeps track of the history of events for security checks and reporting purposes.
Biometrics	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.
Closed system	An environment in which the system access is controlled by persons who are responsible for the content of electronic records that are on the system.
Digital signature	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.
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 computer system.
Electronic signature	The scripted name or legal mark of an individual, handwritten by that individual and executed or adopted with the present intention to authenticate writing in a permanent form.
Instruction sets	Pre-defined sequences of actions or sets of parameters, including measurement programs, automatic processing rules, user batches for automatic analysis and report templates.
Open system	An environment in which the system access is not controlled by persons who are responsible for the content of electronic records that are on the system.
Operating system	Microsoft Windows (or MS Windows): Windows XP, Windows 7, Windows 8 or Windows 10.
Standard operating procedure	A set of standards dedicated to a specific topic. This will define the explicit method(s) to be followed in accomplishing a designated task.
System log	A log that contains system related messages including system error messages.