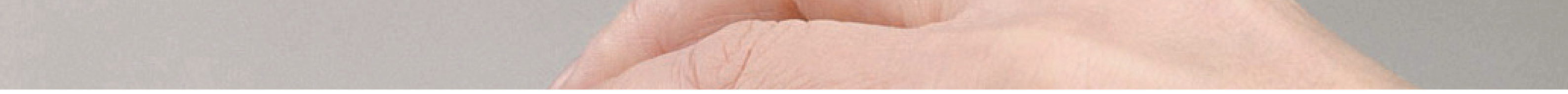

PANalytical
get insight

XRD SYSTEMS

White paper

Supporting the pharmaceutical industry with 21 CFR Part 11 compliance readiness

Table of contents

Edition notice

Fifth Edition, June 2016

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 equipment qualification is supported with products and services.

Complete traceability and reproducibility is guaranteed in terms of experiment (the XRDML data platform stores all details from unique instrument identification down to the last set-up and measurement detail), 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 tamper-proof 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

The XRD systems that are discussed in this document comprise X'Pert PRO MPD, X'Pert Powder systems, Empyrean, X'Pert^3 Powder, CubiX PRO and CubiX^3, each with their instrument control software version and additionally the software packages PANalytical Audit Trail software version 1.4 and higher, Data Collector version 4 and higher, Data Viewer 1.4 and higher, X'Pert Industry version 2 and higher and HighScore (Plus) version 3 and higher, all running on a PC with MS Windows 7 and higher operating system. 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 each software module he wants to use. The following security events are saved into the audit trail: software module login/logoff, start/stop instrument sessions and security alarm events. Additionally in the Alarm Monitor an alarm is generated after three failed attempts for each security or signature event. PANalytical uses the MS Windows user name and passwords. Password length, expiration period, etc. are subject to the MS Windows security policy set-up. Where needed the software modules provide privilege levels, depending on 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

Experimental 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. This is exactly what PANalytical systems do by combining the XRDML data platform, analysis documents, and the audit trail records.

The audit trail records contain data about process, security and electronic record traceability.

The PANalytical audit trail functionality is based on the principle of clients and a server, which enables larger networked systems. The audit trail records are stored in a central server database.

The following events are saved as audit trail records: application login/logoff, unauthorized attempts handling, start/ stop instrument sessions, and new/ changed electronic records.

The audit trail record contains the following data, if applicable: event type, user ID, full (printed) user name, date/ time (including UTC offset), electronic record checksum (Checksum method: RSA MD5 Message Digest 128 bit checksum), electronic record identification, additional data such as sample name and sample ID.

The audit trail software is always active and cannot be bypassed. Even unexpected loss of communication in the LAN does not influence the audit trailing.

The reporting functionality of the audit trail 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 XRD systems electronic records comprise measurement programmes in XRDMP files, measured data in XRDML files, and analysis data in documents using a proprietary format.

Reports can be created as HTML, DOC, RTF, and PDF files depending on the application software. The used file formats are based on standard XML, HTML, DOC and RTF. 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.

All electronic records can be protected from both modification and deletion using the Microsoft Windows data security mechanisms and procedures. Furthermore checksum data is available in the PANalytical Audit Trail software to guarantee data authenticity.

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 PANalytical Audit Trail software. The connection to the electronic record itself is done via the name of the electronic record together with the checksum information. All sessions are treated as continuous sessions. 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 [2]. For each FDA requirement it is explained how this requirement is implemented in PANalytical XRD systems.

Subpart B - Electronic records

Section	Requirement	PANalytical implementation
§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:	The design, development, manufacturing and life cycle management of PANalytical's products is done according to ISO9001 and ISO14001 certified procedures. These products are ready to be integrated in a 21 CFR Part 11 compliant laboratory, providing and guaranteeing authenticity, integrity and confidentiality of electronic records and electronic signatures.
(a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	The system owner is responsible for the validation of the applications and processes. PANalytical gladly offers products and services for system validation support. This includes products for Installation Qualification (IQ) and Operation Qualification (OQ), and support for Design Qualification (DQ) and Performance Qualification (PQ). The PANalytical software detects if electronic records have been changed or made invalid using checksums (RSA MD5 Message Digest 128 bits checksum). Audit trails for logging in/ off and instrument events, as well as events involving electronic records 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.	Electronic records can be copied as files to portable media or network via MS Windows. PANalytical is using a number of file formats among which are a few proprietary formats. The readability of the proprietary formats by the PANalytical software is guaranteed throughout the minimum retention period as required for the subject electronic records. Non-proprietary formats include XML, HTML, DOC, RTF, PDF or plain text. All of these formats are published standards and can be read with any common editor or browser. The audit trail database is not written in a human readable form. Printed reports of all electronic records as well as audit trail records can be obtained. These reports can also be written to human readable file formats.
(c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	The use of checksums (see a) protects electronic records against voluntary and involuntary change. It is the responsibility of the system owner to provide facilities for system security, backing up and archiving as well as disaster recovery not already covered by the PANalytical system.
(d)	Limiting system access to authorized individuals.	The computer provides limited access via the MS Windows operating system and each PANalytical software package has its own secure login functionality. Configuration and maintenance of these is the responsibility of the system owner.

Section	Requirement	PANalytical implementation
(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.	This is the basic functionality of PANalytical Audit Trail software. All security and electronic record related events are stored as audit trail records with the proper operator, actions, date/time, and electronic record and checksum information.
	Record changes shall not obscure previously recorded information.	Measurement data cannot be changed; analysis data has a history log and cannot be overwritten.
	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.	PANalytical Audit Trail software provides database upgrade capabilities, guaranteeing a retention period at least as long as required for the subject electronic records. Reports made by the PANalytical Audit Trail software ensure human readability for reviewing and copying purposes.
(f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	For both measurements and analyses, instruction sets can be pre-defined in the PANalytical systems. This should be done and maintained by the system owner. Data review before analysis is not enforced.
(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 computer provides limited access via the MS Windows operating system, and all PANalytical software modules have their own login functionality, including user privileges or authorization levels. It is the responsibility of the system owner to verify the identity of the individual to whom an electronic signature will be issued.
(h)	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	To ensure validity of data input the diffractometer shouldn't be connected to networked environment as input security cannot be guaranteed. Measurement data traceability includes the unique instrument identification.
(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.	Not applicable. This is the responsibility of the system owner.

Section	Requirement	PANalytical implementation
(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.
§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.	Not applicable. The PANalytical systems are 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.	PANalytical systems support non-biometric electronic signatures. These include: (1) The full user name is available as printed name. (2) The date and time of signing is available including UTC offset indication. (3) The meaning of the signing.
(b)	The items identified in paragraphs (a) (1), (a) (2), and (a) (3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).	The information above (a) is shown both on displayed and on printed copies of the records.
§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.	In PANalytical systems electronic records and electronic signatures are linked via checksum functionality. The method used is: RSA MD5 Message Digest 128 bits checksum. The same is valid for handwritten signatures executed to electronic records containing measured data.

Subpart C – Electronic signatures

Section	Requirement	PANalytical implementation
§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.	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 a proper set-up in MS Windows.
(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. 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. 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.	Not applicable. This is the responsibility of the system owner.
§C11.200	Electronic signature components and controls	
(a)	Electronic signatures that are not based upon biometricsshall: (1) Employ at least two distinct identification components such as an identification code and password. (i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. (ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.	PANalytical systems support non-biometric electronic signatures. (1) Signing always requires a combination of user name and password that is enforced to be unique by the system. (i) For signings during a single, continuous period of controlled system access, the first signing is executed using both electronic signature components; subsequent signings use only the password. (ii) Not applicable. Logging in to a PANalytical software module marks the start of a single, continuous period of controlled system access, while logging off marks the end of this period.

Section	Requirement	PANalytical implementation
	(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.	(2) Not applicable. This is the responsibility of the system owner. (3) No individual is able to read the password of any user.
(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. PANalytical does not support biometric 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:	PANalytical software uses the functionality available in the MS Windows operating system.
(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 MS Windows 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 MS Windows operating system. The set-up and maintenance is the responsibility of the system owner.
(c)	Following loss management procedures to electronically de-authorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information. And to issue temporary or permanent replacements using suitable, rigorous controls.	In PANalytical systems MS Windows 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. If the number of unsuccessful attempts is exceeded an alarm is sent to pre-defined locations. 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
CMM	Capability Maturity Model
DQ	Design Qualification
FDA	Food & Drug Administration
G*P	Good Laboratory/Manufacturing/Automated Manufacturing/etc. Practice
HTML	Hyper Text Markup Language
IQ	Installation Qualification
IP	Internet Protocol
ISO	International Organization for Standardization
LAN	Local Area Network
MPD	Multi-purpose Diffractometer
MS	Microsoft
PC	Personal Computer
PDF	Portable Document Format
PQ	Performance Qualification
OECD	Organization for Economic Co-operation and Development
OQ	Operation Qualification
RTF	Rich Text File
SOP	Standard Operating Procedure
UTC	Universal Coordinated Time
XML	Extensible Mark-up Language
XRD	X-ray Diffraction

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.
Checksum	Number calculated according to an algorithm that takes the file contents (partly or complete) into account. This number is used for the authenticity check.
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 7 or Windows 8.1.
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.
XRDML	The PANalytical XRD data platform for measured data, based on XML technology.