System Assessment Report

Relating to Electronic Records and Electronic Signatures;

Final Rule, 21 CFR Part 11

System: PC Control 6.0 for Titrando

1 Procedures and Controls for Closed Systems

run no.	Ref.	Topic	Question	Yes	No	partly	Comments
1.1	11.10 (a)	Validation, IQ, OQ	Is the system validated?	**O**			The operator is solely responsible for the validation of the system. The responsibility of the supplier lies in supplying systems which are capable of being validated. This is supported by the internal Metrohm quality control system which can be audited at any time. In this respect Metrohm offers a range of validation services: conformity certificates, prepared documentation for IQ and OQ, carrying out IQ and OQ at the operator's premises,... Standard methods for system validation are stored in the system.
1.2	11.10 (a)	Audit Trail, Change	Is it possible to discern invalid or altered records?	**X**			All relevant operator entries are recorded in an automatically generated audit trail together with date, time with difference to UTC (Coordinated Universal Time) and user. In the report any altered results data (results) is indicated by the comment "recalculated on/by". For method alterations the altered version is indicated by having the status "modified". In case of saving an altered method or altering result data (recalculation) a reason plus a comment can be entered. A version check is implemented for all files (methods, determinations, ...). This means that altered data lead to the creation of a new file, which can be saved with a new, version-guided name. Invalid results can be recognized if limits have been defined. If these are infringed then the result will be marked and a message will be produced.

run no.	Ref.	Topic	Question	Yes	No	partly	Comments
1.3	11.10 (b)	Report, Printout, Electronic Record	Is the system capable of producing accurate and complete copies of electronic records on paper?	**X**			Configurable reports can be printed out for methods and determinations (results data). Alterations to the report configuration can be disabled for routine users. The automatic printout at the end of an analysis can be stipulated by system settings in the system. In this way it can be ensured that the operator of the system can reliably follow any alteration, overwriting or deletion of the data of a determination. Each printout is accompanied by a time stamp giving information about the time with difference to UTC (Coordinated Universal Time).
1.4	11.10 (b)	Report, Electronic Record, FDA	Is the system capable of producing accurate and complete copies of records in electronic form for inspection, review, and copying by the FDA?	**X**			All data is stored in formatted ASCII-format as a PC/LIMS report. The automatic printout at the end of an analysis can be stipulated by system settings in the instrument. In this way it can be ensured that the operator of the system can reliably follow any alteration, overwriting or deletion of the data of a determination.
1.5	11.10 (c)	Electronic Record, Retention Period, Archiving	Are the records readily retrievable throughout their retention period?	**O**			The operator is solely responsible for storage/archiving. The system can permanently store the data by using an archiving system or on a network drive or on paper. The data on the data carrier is encrypted and provided with a checksum. In this way it is protected against accidental and improper alteration. Alterations are recognized by the system. The contents can be read out at any time by the PC Control Software. The method used for archiving data together with the data to be archived must be defined by the operator. Interfaces for archiving (PC/LIMS) are present in the system.

run no.	Ref.	Topic	Question	Yes	No	partly	Comments
1.6	11.10 (d)	Login, Access Protection, Authorization User, Administrator	Is the system access limited to authorized individuals?	**X**			The system is provided with a login system with 3 internal access levels (Administrator, Expert, Routine user). If identification cards are used then an infinite number of intermediate levels can be configured, see also 11.10 (g), No. 1.12. The person responsible for the system (Administrator) must ensure that only authorized persons are assigned rights of access.
1.7	11.10 (e)	Audit Trail, Electronic Record, Operator Entries	Is there a secure, computer generated , time stamped audit trail that records the date and time of operator entries and actions that create, modify, or delete electronic records?	**X**			All relevant operator entries are recorded in an automatically generated audit trail together with date, time with difference to UTC and user.
1.8	11.10 (e)	Electronic Record, Overwriting data, Change	Upon making a change to an electronic record, is previously recorded information still available (i.e., not obscured by the change)?			**X**	No, the system overwrites the information in the internal memory. If data is altered and saved then a new version will be created automatically; however, this overwrites the previous version. A) Can only be ensured organizationally that, after the alteration, a file with an unambiguous file name is stored and archived. B) Can only be ensured organizationally that the paper-based printouts of the methods and determinations are produced and managed.
1.9	11.10 (e)	Audit Trail, Retention Period	Is an electronic record's audit trail retrievable throughout the record's retention period?	**X**			As long as the audit trail has not been deleted it persists. The disk space is the limiting factor here. The audit trail can only be deleted after it has been exported. The operator is solely responsible for storage/archiving after export.
1.10	11.10 (e)	Audit Trail, FDA, Inspection	Is the audit trail available for review and copying by the FDA?	**X**			The audit trail can be exported as text file. Thus it is available in electronic form and on paper. Furthermore a protected audit trail can be generated in form of a PDF file.

run no.	Ref.	Topic	Question	Yes	No	partly	Comments
1.11	11.10 (f)	Sequence of steps, Plausibility Check, Devices	If the sequence of system steps or events is important, is this enforced by the system (e.g., as would be the case in a process control system)?	**X**			Plausibility checks are carried out by the system when a determination is started, for example, a check is made whether all the necessary instruments are present. The determination sequence is programmed in the method and must be strictly observed. The observation of the sequence is supported by the use of sample assignment table and automatic sample data request. Only those functions that can actually be carried out are accessible.
1.12	11.10 (g)	Login, Access Protection, Authorization, User, Administrator	Does the system ensure that only authorized individuals can use the system, electronically sign records, access the operation, or computer system input or output device, alter a record, or perform other operations?	**X**			The user can be identified by the login function. (The person responsible for the system (Administrator) must ensure that only authorized persons are assigned rights of access.) The Administrator function can be clearly separated from user roles, see also 11.10 (d), No. 1.6. Methods and determinations can be signed and therefore can be electronically released. There are two signature levels. The system demands that the reviewing and the releasing person are not the same.
1.13	11.10 (h)	Balance, Connection, Terminals, Input data, Devices	Does the system control validity of the connected devices? *If it is a requirement of the system that input data or instructions can only come from certain input devices (e.g., terminals) does the system check the validity of the source of any data or instructions received? (Note: This applies where data or instructions can come from more than one device, and therefore the system must verify the integrity of its source, such as a network of weigh scales, or remote, radio controlled terminals).*	**X**			During the IQ all the connected instruments are entered in the list of devices and subsequently checked. For barcode scanners the system setting "Input target" must be checked and the barcode scanner set correctly (IQ). Metrohm instruments are recognized, their validity is checked and they are entered in the list of devices. Balance: the configuration of the balance is stored in the system. In order to check that the correct balance is actually connected the operator must carry out an IQ after a system installation or alteration. The obtained data is checked for the correct identification and the position of the weight in the character sequence. No further check of the contents is possible. Validation of the connected devices is carried out within the framework of the system validation (see also 11.10 (a), No. 1.1).

run no.	Ref.	Topic	Question	Yes	No	partly	Comments
1.14	11.10 (i)	Training, Support, User, Administrator	Is there documented training, including on the job training for system users, developers, IT support staff?	**O**			The operator is responsible for training. Metrohm offers standard training courses for all application sectors. Individual training courses can be specially arranged. Metrohm's product developers and service personnel receive further training at regular intervals.
1.15	11.10 (j)	Policy, Responsibility, Electronic Signature	Is there a written policy that makes individuals fully accountable and responsible for actions initiated under their electronic signatures?	**O**			If an electronic signature is used then the operator must have a policy in which the equality of handwritten and electronic signatures is made clear.
1.16	11.10 (k)	Documentation, Distribution of Documentation, Access to Documentation, System Documentation, Logbook, Manuals	Is the distribution of, access to, and use of systems operation and maintenance documentation controlled?	**O**			The system has a comprehensive online help system that supports the user and the service personnel. Distribution of paper-based documentation is the responsibility of the operator.
1.17	11.10 (k)	SOP, Documentation, Manuals, System Documentation, Audit Trail , Logbook	Is there a formal change control procedure for system documentation that maintains a time sequenced audit trail for those changes made by the pharmaceutical organization?	**O**			Supported by clear system assignment and version of the documentation. However, the operator must maintain a device logbook and note any alterations to the documentation and software. Forms for these documents are supplied by Metrohm.

2 Additional Procedures and Controls for Open Systems

run no.	Ref.	Topic	Question	Yes	No	partly	Comments
2.1	11.30	Data, Encryption, Data Transfer	Can methods and determinations be sent securely to another system? Is data encrypted?	**N/A**			Access to *PC Control* via Internet is not provided. The data is stored as a file, encrypted and provided with a checksum. This means that the data is protected against unauthorized alteration. If an alteration is made then the data is unusable. If faulty data is transferred to a different system this will also be recognized.
2.2	11.30	Electronic Signature	Are digital signatures used?	**N/A**			Access to *PC Control* via Internet is not provided. Methods and determinations can be signed and therefore electronically released. There are two signature levels. The system demands that the reviewing and the releasing person are not the same.

3 Signed Electronic Records

run no.	Ref.	Topic	Question	Yes	No	partly	Comments
3.1	11.50	Electronic Signature	Do signed electronic records contain the following related information? - The printed name of signer - The date and time of signing - The meaning of the signing (such as approval, review, responsibility)	**X**			In case of methods and determinations all signatures contain the full name of the signer, date, time of signing and the reason for signing (from a selection list). Additionally, with the signature, a comment can be entered which is saved with the electronic signature. User data and the audit trail do not have to be signed and therefore are not signed.
3.2	11.50	Electronic Signature	Is the above information shown on displayed and printed copies of the electronic record?	**X**			The report on the screen and on the printout contains signature data.
3.3	11.70	Electronic Signature	Are signatures linked to their respective electronic records to ensure that they cannot be cut, copied, or otherwise transferred by ordinary means for the purpose of falsification?	**X**			The signature is inseparably linked to the method or determination. Therefore falsifying is impossible.

4 Electronic Signature (General)

run no.	Ref.	Topic	Question	Yes	No	partly	Comments
4.1	11.100 (a)	Electronic Signature	Are electronic signatures unique to an individual?	**X**			Yes, by unique relation within the system between user name and individual. It must be assured, at operational level, that user names are only used once.
4.2	11.100 (a)	Electronic Signature	Are electronic signatures ever reused by, or reassigned to, anyone else?	**O**			A used login name is assigned to a person. It must be assured, at operational level that this login name is not assigned to another person. A reactivation is not concerned.
4.3	11.100 (a)	Electronic Signature	Does the system allow the transfer of the authorization for electronic signatures?	**O**			Proxy persons have to be appointed by the administrator. Rules at operational level are required.
4.4	11.100 (b)	Electronic Signature	Is the identity of an individual verified before an electronic signature is allocated?	**O**			By the course of the application it has to be assured, at operational level, that the person that applies is the correct person.

5 Electronic Signatures (Non-biometric)

run no.	Ref.	Topic	Question	Yes	No	partly	Comments
5.1	11.200 (a) (1)(i)	Electronic Signature	Is the signature made up of at least two components, such as an identification code and password, or an id card and password?	**X**			Yes.
5.2	11.200 (a) (1)(ii)	Electronic Signature	When several signings are made during a continuous session, is the password executed at each signing? (Note: both components must be executed at the first signing of a session).	**X**			The password has to be entered with each signature.
5.3	11.200 (a) (1)(iii)	Electronic Signature	If signings are not done in a continuous session, are both components of the electronic signature executed with each signing?	**X**			The password has to be entered with each signature.
5.4	11.200 (a) (2)	Electronic Signature	Are non-biometric signatures only used by their genuine owners?	**O**			The operator has to ensure that a user only uses his own signature.
5.5	11.200 (a) (3)	Electronic Signature, Falsify Electronic Signature	Would an attempt to falsify an electronic signature require the collaboration of at least two individuals?	**X**			Only administrator and user together.

6 Electronic Signatures (biometric)

run no.	Ref.	Topic	Question	Yes	No	partly	Comments
6.1	11.200 (b)	Electronic Signature, Biometric Electronic Signature	Has it been shown that biometric electronic signatures can be used only by their genuine owner?	**N/A**			No biometric electronic signature.

7 Controls for Identification Codes and Passwords

run no.	Ref.	Topic	Question	Yes	No	partly	Comments
7.1	11.300 (a)	Identification Code, Uniqueness, Password, Identification, Login, Access Protection	Are controls in place to maintain the uniqueness of each combined identification code and password, such that no individual can have the same combination of identification code and password?	**X**			The system ensures that each identification code (user name) is only used once within the system; similarly a combination of identification code and password can only occur once. Name alterations must be organizationally managed by the operator! The operator must organizationally ensure that the identification codes are identical for all systems, as otherwise the unambiguity of the users cannot be guaranteed. It is recommended that unambiguous identification codes (e.g. personnel number or initials) covering all systems are used throughout the whole organization. In general it is recommended that guidelines are drawn up for the whole organization in which the creation of user accounts and the use of passwords (length, period of validity,...) are defined.
7.2	11.300 (b)	Identification Code, Password, Validity, Identification, Login, Access Protection	Are procedures in place to ensure that the validity of identification code is periodically checked?	**O**			The operator is responsible for checking the identification codes. The Administrator can print out a list of all the users for this purpose.
7.3	11.300 (b)	Password, Validity, Password Expiry, Identification, Login, Access Protection	Do passwords periodically expire and need to be revised?	**X**			The period of validity for the password can be defined by the Administrator. Values between 30 and 90 days are advisable. A long period of validity represents a security risk. A period of validity which is too short means that the user must frequently remember a new password and may write it down. The system saves the password history and therefore a reuse of passwords is impossible.
7.4	11.300 (b)	Identification Code, Password, Validity, Disable User Access, Identification, Login, Access Protection	Is there a procedure for recalling identification codes and passwords if a person leaves or is transferred?	**O**			The method must be defined by the operator. The Administrator can deactivate the corresponding user in the system.

run no.	Ref.	Topic	Question	Yes	No	partly	Comments
7.5	11.300 (c)	Identification Code, Password, Validity, Disable User Access, Identification, Login, Access Protection, Loss of ID card	Is there a procedure for electronically disabling an identification code or password if it is potentially compromised or lost?	**O**			The method must be defined by the operator. The Administrator can deactivate the corresponding user in the system.
7.6	11.300 (d)	Unauthorized Use, Login, Access Protection	Is there a procedure for detecting attempts at unauthorized use and for informing security?	**X**			After n incorrect attempts (the number can be defined by the Administrator) a message is produced saying that the maximum number of login attempts has been reached and the user is disabled. The message can be sent as an e-mail via a PC with Internet access.
7.7	11.300 (d)	Unauthorized Use, Login, Access Protection	Is there a procedure for reporting repeated or serious attempts at unauthorized use to management?	**O**			A method for reporting such attempts to the Management must be defined by the operator. After n incorrect attempts (the number can be defined by the Administrator) a message is produced saying that the maximum number of login attempts has been reached and the user is disabled. The message can be sent as an e-mail.
7.8	11.300 (c)	Loss of ID card, ID card, Unauthorized Use, Access Protection	Is there a loss management procedure to be followed if a device for identification (e.g. ID card) is lost or stolen?	**O**			The operator is responsible for checking the correct use of identification cards and for the measures to be taken on misuse.
7.9	11.300 (c)	Loss of ID card, Electronically Disabling ID card, ID card, Unauthorized Use, Access Protection	Is there a procedure for electronically disabling a device if it is lost, or stolen, or potentially compromised?	**O**			The operator is responsible for checking the correct use of identification cards and for the measures to be taken on misuse. The card itself cannot be disabled. However the authorized user of the card can be disabled in the system. This is the operator's responsibility.
7.10	11.300 (c)	ID card, Access Protection	Are there controls over the issuance of temporary and permanent replacements?	**O**			The operator is responsible for checking the correct use of identification cards and for the use of replacement cards. A copy of an identification card does not represent a security risk if the system information it contains is up to date.
7.11	11.300 (e)	Testing of ID cards, ID card, Access Protection	Is there initial and periodic testing of tokens and cards?	**O**			The operator is responsible for checking the correct use of identification cards and for checking their correct functioning at regular intervals.

run no.	Ref.	Topic	Question	Yes	No	partly	Comments
7.12	11.300 (e)	Modification of ID cards, ID card, Unauthorized Use, Access Protection	Does this testing check that there have been no unauthorized alterations?	**O**			The operator is responsible for checking the correct use of identification cards and for checking their correct functioning at regular intervals. The system can detect whether the data contained on the card has been modified, as all data is encrypted and provided with a checksum on storage. This means that it can always be ensured that no unauthorized alterations have been carried. Alteration of the data by the system can only be carried out by the Administrator.

O = The operator is responsible.
N/A = Not Applicable

A physical audit has been performed on the base of the Version 3.0 on the 02.03.2004. According to Metrohm Ltd., the implemented changes in the current version are not relevant regarding 21 CFR Part 11 (see Release Notes 8.840.8009EN). Therefore this update was carried out without a physical audit.

8 Indices

Reference to the page number:

Reference to the run number of the entry: