System Assessment Report

Relating to Electronic Records and Electronic Signatures;

21 CFR Part 11

System: 900 Touch Control
(Software version 5.900.0032)

1 Procedures and Controls for Closed Systems

Run no.	Ref.	Topic	Question	Yes	No	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 management 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, performing 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 login name. The audit trail is stored internally and can be copied to an USB stick via backup function. The audit trail can be examined using the Audit Trail Viewer. In the report any altered results data (results) are 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. 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 displayed.

Run no.	Ref.	Topic	Question	Yes	No	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 forced by system settings. In this way it can be ensured that the operator of the system can reliably track 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 forced by system settings. In this way it can be ensured that the operator of the system can reliably track 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 record storage/archiving. The system can store permanently the records on an USB stick, by using an archiving system 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 Touch Control software. The method used for archiving data together with the definition which data to be archived must be defined by the operator. Interfaces for archiving (USB stick or PC/LIMS) are present in the system.
1.6	11.10 (d)	Login, Access Protection, Authorization User, Administrator	Is the system access limited to authorized individuals?	**X**		The system provides a login system with three 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 access rights are granted to authorized persons only.

Run no.	Ref.	Topic	Question	Yes	No	Comments
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 login name. The audit trail is stored internally and Clinical Analyzer be copied via backup function to an USB stick. The audit trail can be examined using the Audit Trail Viewer.
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)** **O**		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. Organizational safeguards have to be implemented to ensure that, after the alteration, a file with an unambiguous file name is stored and archived. If printouts exist of the electronic records, organizational safeguards have to be implemented to ensure that, after the alteration, printouts of the respective methods and determinations can be - identified unambiguously - refer to the correct methods and determinations.
1.9	11.10 (e)	Audit Trail, Retention Period	Is the audit trail of an electronic recording retrievable throughout the retention period of the respective record?	**(X)** **O**		The audit trail is stored internally and can be copied to an USB stick via backup function. The audit trail can be examined using the Audit Trail Viewer. 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 an text file using the Audit Trail Viewer software that is delivered with Touch Control system. Thus it is available in electronic form and on paper. Furthermore a protected audit trail can be generated by means of a PDF file.
1.11	11.10 (f)	Control over 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 it 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 necessary devices are present. The sequence of the determination is programmed in the method and must be strictly maintained. Maintaining the sequence is supported by using the sample assignment table or the automatic sample data request. Only the functions to be carried out are accessible.

Run no.	Ref.	Topic	Question	Yes	No	Comments
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 access rights are granted to authorized persons only.) 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 be released electronically. There are two signature levels. The system demands that the reviewing and the releasing person is 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/O**		USB instruments, e. g. printers, barcode scanners and keyboards, are recognized and their validity is checked. The vendor-ID is automatically read off and inserted automatically in the list of devices. During the IQ all the connected instruments are entered into the list of devices and checked subsequently. For barcode scanners the system setting "Input target" must be checked and the barcode scanner set accordingly (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 modification. The data obtained is checked for the correct identification and position of the weight in the character sequence. There is no further check of the content. Qualification of the connected instruments is carried out as part of the system validation (see also 11.10 (a), No. 1.1) which is part of the operator's responsibility.
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?	**X/O**		The operator is responsible for user training and the supporting staff. Metrohm offers standard training courses for all application fields. Individual training courses can be arranged separately. Metrohm's product developers and service personnel receive further training on regular intervals.

Run no.	Ref.	Topic	Question	Yes	No	Comments
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 place 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 in 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?	**X/O**		The system documentation is unambiguously assigned to a particular system and software version. Release notes are kept with each software version. However, the operator must maintain records about documentation and system changes – e. g. in the device logbook. Templates of these documents are supplied by Metrohm.

2 Additional Procedures and Controls for Open Systems

Run no.	Ref.	Topic	Question	Yes	No	Comments
2.1	11.30	Data, Encryption, Data Transfer	Can methods and determinations be sent securely to another system? Is data encrypted?	**N/A**		*900 Touch Control* is not designed to be accessed via the Internet. The data are stored as a file, encrypted and provided with a checksum. This protects the data against unauthorized modification. In case of a modification the data become useless. Even if corrupted data are transferred to another system this is recognized.
2.2	11.30	Electronic Signature	Are electronic signatures used?	**N/A**		*900 Touch Control* is not designed to be accessed via the Internet. There are two signature levels. Methods and determinations can be signed and with that - electronically approved. The system demands that the reviewing and the releasing person is not the same.

3 Signed Electronic Records

Run no.	Ref.	Topic	Question	Yes	No	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 and time of the signature and the meaning (out of a list box) of the signature. Additionally, a comment on a signature can be entered, which is saved together with the electronic signature.
3.2	11.50	Electronic Signature	Is the above information shown on displayed and printed copies of the electronic record?	**X**		Full signature data are shown on the display and on printouts.
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 securely linked to the respective method or determination. Signature elements cannot be cut, copied or transferred by ordinary means. User information is completely integrated in the signature. When displaying the signature, this information is always readable in plain text.

4 Electronic Signature (General)

Run no.	Ref.	Topic	Question	Yes	No	Comments
4.1	11.100 (a)	Electronic Signature	Are electronic signatures unique to an individual?	**X**		Each user gets a unique login name. It must operationally be ensured, that user login names are used only once (the system monitors the unambiguousness of the login name).
4.2	11.100 (a)	Electronic Signature	Are electronic signatures ever reused by, or reassigned to, anyone else?	**O**		A login name used is assigned to one person. It must operationally be ensured, that this login name is not assigned to another person. A reactivation is not affected by this.
4.3	11.100 (a)	Electronic Signature, Representative	Does the system allow the transfer of the authorization for electronic signatures (representatives)?	**O**		Secure and traceable user rights management is in the responsibility of the user. The assignment of representatives is part of the regular user management and has to be carried out by the administrator. A procedure has to be in place for this.
4.4	11.100 (b)	Electronic Signature	Is the identity of an individual verified before an electronic signature is allocated?	**O**		With the initial assignment of signing rights to a user, the identity of the respective person has to be verified against the user rights request.

5 Electronic Signatures (Non-biometric)

Run no.	Ref.	Topic	Question	Yes	No	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**		The signing function is carried out with login name and password.
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 login name and the password have 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 uses his/her own signature only.
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**		Nobody has access to the electronic signature data by ordinary means.

6 Electronic Signatures (biometric)

Run no.	Ref.	Topic	Question	Yes	No	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 electronic signature based on biometric means.

7 Controls for Identification Codes and Passwords

Run no.	Ref.	Topic	Question	Yes	No	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 login name) is used only once within the system and therefore each combination of identification code and password can also exist only once. Alterations of names must be 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) are used for all systems 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 periodically; this can be supported by a system function which allows the administrator to print out a list of all the registered users.
7.3	11.300 (b)	Password, Validity, Password Expiry, Identification, Login, Access Protection	Do passwords periodically expire and need to be revised?	**X**		The validity period of the password can be defined by the administrator. Values between 30 and 90 days are common. After this period is expired, the user is forced to change his/her password. The system saves the password history and prevents the user from re-using a password.
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 procedure has to be set up by the operator. The corresponding user account can be disabled in the system by the administrator, but remains saved in the system as part of the group "removed users" without any access rights.

Run no.	Ref.	Topic	Question	Yes	No	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 procedure has to be set up by the operator. The administrator can disable the corresponding user account in the system.
7.6	11.300 (c)	Loss of / compromised ID card, Electronically Disabling ID card	Is there a procedure for electronically disabling a device if it is lost, or stolen, or potentially compromised?	**N/A**		There is no hardware device for user identification.
7.7	11.300 (c)	ID card, Replacement	Are there controls over the temporary or permanent replacement of a device?	**N/A**		There is no hardware device for user identification.
7.8	11.300 (d)	Unauthorized Use, Login, Access Protection	Are there security safeguards in place to prevent and/or detect attempts of unauthorized use of user identification or password?	**X/O**		After *n* incorrect attempts (number can be defined by the administrator) a message is displayed, saying that the maximum number of unsuccessful login attempts has been reached and the user account is disabled. A corresponding message can be sent to the management by EMail.
7.9	11.300 (d)	Unauthorized Use, Login, Access Protection, Inform management	Is there a procedure in place to inform the responsible management about unauthorized use of user identification or password?	**O**		The procedure to inform the security manager has to be implemented by the operator.
7.10	11.300 (e)	Testing of ID cards, ID card, Access Protection	Is there initial and periodic testing of tokens and cards?	**N/A**		There is no hardware device for user identification.
7.11	11.300 (e)	Modification of ID cards, ID card, Unauthorized Use, Access Protection	Does this testing check that there have been no unauthorized alterations?	**N/A**		There is no hardware device for user identification.

O = Implementation is in the operator's responsibility
N/A = Not Applicable to the system

This 21 CFR Part 11 assessment is based on a physical audit performed March the 2nd 2004. Subject of this audit was the software version 5.840.0120. According to Metrohm AG management (development and QA) all implemented changes in the following versions – including the current version – are not relevant with regard to 21 CFR Part 11 or 21 CFR Part 11 compliant (see Release Notes 8.840.8009EN, 8.900.8004EN, 8.900.8009EN, 8.900.8016EN, 8.900.8017EN, 8.900.8019EN, 8.900.8021EN). Therefore, this update does not require a physical re-audit.

8 Indices

Reference to the page number:

Reference to the run number of the entry: