System Assessment Report

Relating to Electronic Records and Electronic Signatures;

21 CFR Part 11

System: 916 Ti-Touch
(Firmware version 5.916.0040)

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 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 on request. Metrohm offers a range of validation services: conformity certificates, documentation for IQ/OQ procedures, and support for performing IQ/OQ at the operator's site. 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's entries are recorded in an automatically generated audit trail together with date and time (according to ISO 8601) – including the time difference to UTC[1] - and user identification. The audit trail is stored internally and can be copied to a USB storage medium using the backup function. The content of the audit trail can be examined using the Audit Trail Viewer software. Any determination[2] modification is indicated in the audit trail report by the fields "recalculated on" and "recalculated by". New method versions are labelled with the status "modified" in the audit trail report. The user is asked to select a reason (via dropdown list) when he/she wants to save a modified method or determination (after recalculation); Additionally a comment can be entered. Invalid results can be recognized if result limits have been defined. If such a limit is violated, the respective result will be marked with a special color and a corresponding message is saved in the determination. The action to be carried out when the result limits are exceeded can be defined.

[1] UTC: Coordinated Universal Time (English), Temps universel coordonné (French)
[2] The determination data set includes the result data.

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, determinations and system configuration. Modification of the report configuration can be disabled for routine users. Automatic printout at the end of an analysis can be defined in the method. 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.
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**		Determinations can be stored as PC/LIMS report in ISO/IEC 8859-1 (txt) or UTF-8 format. There is a method option which – when set – generates an automatic printout at the end of an analysis. 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. All data (methods, determinations, audit trail[3]) can be printed in PDF format.
1.5	11.10 (c)	Electronic Record, Retention Period, Archiving	Are the records readily retrievable throughout their retention period?	**X/O**		The operator is responsible for record storage/archiving. Electronic records (methods, determinations and settings) can be archived using the backup function (filing on a USB storage medium) or printing them.[4] The data on the medium are coded in binary format and provided with a checksum. In this way it is protected against accidental and improper alteration. Alterations are recognized by the system. Data on the medium can be retrieved at any time with help of any Touch Control device. The operator has to define the archiving method as well as the data to be archived. Interfaces for archiving (USB storage medium, PDF file or PC/LIMS report) are present in the system.

[3] Printing audit trail information requires backup on a USB drive first and import into the Audit Trail Viewer software.
[4] In contrast to the PDF reports the PC/LIMS report is a plain text file without any format-based integrity checks.

Run no.	Ref.	Topic	Question	Yes	No	Comments
1.6	11.10 (d)	Login, Access Protection, Authorization User, Administrator	Is the system access limited to authorized individuals?	**X**		The system has three internal (built-in) access roles (Administrator, Expert and Routine User). Using identification profiles[5] allow configuring an infinite number of dedicated, tailored roles (please refer also to no. 1.12, Ref.11.10 (g)). The person responsible for the system (e.g., Process Owner) must ensure that access rights are granted to authorized persons only.
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? Does the audit trail (mandatorily) collect the reason for a record change or deletion?	**X**		All relevant operator entries are recorded in an automatically generated audit trail together with date and time (according to ISO 8601) – including the time difference to UTC[1] - and user identification. The audit trail is stored internally and can be copied to a USB storage medium using the backup function. The content of the audit trail can be examined using the Audit Trail Viewer software. Record changes require the user to select a reason from a drop-down list; optionally an additional comment can be entered.
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 data in the internal memory. If data is altered and then saved, a new record version is created automatically which overwrites the previous version. Starting from a defined record template all modifications are fully traceable in the audit trail. When creating a new method, all entered commands are recorded in the audit trail; parameter changes are recorded in the audit trail also. Similarly modifications of a determination are recorded in the audit trail too. So the previously entered data is still available and recorded in the audit trail. It is recommended to have organizational safeguards in place which instruct the operator to store and archive the respective electronic record with an unambiguous file name prior to the modification. It is recommended to instruct the operator to add 'Determination properties' to the report templates; doing so the determination version is printed on the report. So printouts on paper or PDF documents of different record versions on paper and/or electronically are always transparent and traceable.

[5] Identification profiles are to be stored on a USB drive and contain user credentials and access rights which are read during login.

Run no.	Ref.	Topic	Question	Yes	No	Comments
1.9	11.10 (e)	Audit Trail, Retention Period	Is the audit trail of an electronic record retrievable throughout the retention period of the respective record?	**X/O**		The audit trail is stored internally and can be copied to a USB storage medium using the backup function. The content of the audit trail can be examined using the Audit Trail Viewer software. The operator is responsible for storage/archiving after the audit trail 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 a text file using the Audit Trail Viewer software which is delivered on a USB storage medium with the Touch Control device. Thus the audit trail is available in electronic form and as printout. Furthermore a protected[6] audit trail can be generated as 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 a determination is programmed in the method and is strictly maintained; in addition critical operational aspects are time monitored by the system (e.g., monitoring of sensor calibration, titer determination, or reagent). Maintaining the sequence of the samples' analysis is supported by using the sample assignment table or the automatic sample data request. Only the functions to 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 (e.g. Process Owner) must ensure that access rights are granted to authorized persons only. The administrator function can be clearly separated from user roles (please refer to no. 1.6, Ref. 11.10 (d)). Methods and determinations can be signed and therefore released electronically. There are two signature levels: review (signature level 1) and release (signature level 2). The system controls that the individuals who review and release the electronic record are not the same person.

[6] The generated PDF is protected against modification by means of an automatically generated password.

Run no.	Ref.	Topic	Question	Yes	No	Comments
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**		Metrohm instruments are recognized and configured automatically; their validity is checked and they are automatically entered in the 'Device manager' list. USB connected instruments, e.g., barcode scanners or keyboards have to be inserted manually in the 'Device manager' list. During IQ all connected instruments are entered into the list of devices and checked subsequently. For barcode scanners the system setting "Barcode input target" must be checked and the barcode scanner set accordingly (IQ)[7]. Balance (RS-232 device): 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 the system installation or a 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 (please refer to no. 1.1, Ref. 11.10 (a)), which is in 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 the training of the users and of 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 training on a regular basis; particularly quality staff gets regularly training on selected GxP topics.
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.

[7] This setting is not available to the routine user.

Run no.	Ref.	Topic	Question	Yes	No	Comments
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 supporting the user and the service personnel. Additionally, service technicians have access to online service documentation. Distribution of printouts of the 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 (= version history) for creation and modification?	**X/O**		The user manual is unambiguously assigned to a particular firmware version. Release notes are published for each firmware version, which describe the differences to the previous version. However, the operator must maintain records about documentation and system changes as part of the regular change management process.

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**		The 916 Ti-Touch is not designed to be accessed via the Internet. The data are stored as a file, encrypted and provided with a check-sum. This protects the data against unauthorized modification. In case of an irregular modification the data cannot processed any more. Even if corrupted data are transferred to another system this is recognized.
2.2	11.30	Electronic Signature	Are digital signatures used to authenticate involved parties?	**N/A**		The 916 Ti-Touch is not designed to be accessed via the Internet. There are two signature levels for review and approval of methods and determinations. The system controls that the individuals who review and release the electronic record are not the same person.

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**		Signed methods and determinations contain the full name of the signer, date and time of the signature and the meaning of the signature (to be chosen out of a drop-down list) for the signature. In addition a comment can be added to the signature, 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**		Signature data are shown completely 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.

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/O**		Each user gets unique user identification. It must operationally be ensured, that a user identification is assigned to a single person and not to a user group (i.e. group account). The system monitors the unambiguousness of the user identification.
4.2	11.100 (a)	Electronic Signature	Are electronic signatures ever reused by, or reassigned to, anyone else?	**O**		User identification must be assigned just to one individual. It must operationally be ensured that this user identification is not assigned to another individual. Reactivation of a deactivated account 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 (to representatives)?	**O**		Secure and traceable user administration is in the responsibility of the operator. 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 assigned?	**O**		With the initial signing rights assignment 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 user identification and password.[8]
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**		User identification and password have to be entered with each signature.[9]
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**		User identification and password have to be entered with each signature.[9]
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 credentials 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.

[8] There is an administrative setting whether access control requires a password or not; this applies to identification profiles also.
[9] There is no function like 'Signing in a continuous session'.

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 by their genuine owner only?	**N/A**		The electronic signature is not based on biometrics.

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 identification) is used only once within the system - therefore each combination of identification code and password can also exist only once. Alterations of names must be managed by the operator. 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 password complexity requirements (length, period of validity, etc.) 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 is supported by a system function which allows the administrator to print 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 in the password options. According to the setting 'Password expires every *n* days' the user is forced to change his/her password. The system maintains a 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 administrator can set the status of the corresponding user account to 'inactive', which disables the user's system access.
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 set the status of the corresponding user account to 'inactive', which disables the user's system access.

Run no.	Ref.	Topic	Question	Yes	No	Comments
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?	**O**		The operator is responsible for managing the use of identification profiles and to prevent the use of potentially compromised identification profiles (e.g., by setting the respective user account to 'inactive'[10]).
7.7	11.300 (c)	ID card, Replacement	Are there controls over the temporary or permanent replacement of a device?	**O**		The operator is responsible for managing the safe use of identification profiles; this includes in particular control over copies of the identification profiles stored on USB storage mediums. The operator is responsible for checking the correct use of identification profiles and for the measures to be taken on misuse. The identification profile itself cannot be disabled. However the user of this profile can be disabled in the user administration. The operator solely is responsible for this.
7.8	11.300 (d)	Unauthorized Use, Log-in, 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 a defined number of incorrect attempts (the maximal number of entry attempts can be defined by the administrator in the password options) 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, Log-in, 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?	**X/O**		The integrity of the identification profile on the USB storage medium is protected by a checksum – so it is checked with every login. The operator is responsible to verify the authorization on a regular basis (e.g. as part of the Periodic Evaluation/Periodic Review).
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?	**X/O**		The integrity of the identification profile on the USB storage medium is protected by a checksum – so it is checked with every login. The operator is responsible to verify the authorization on a regular basis (e.g. as part of the Periodic Evaluation/Periodic Review).

[10] Identification codes itself cannot be disabled.

Legend

X	Applies to system
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 remote audit performed on May 8th, 2017. Subject of this audit was the firmware version 5.916.0040 with all compliance features enabled.

8 Indices

Reference to the page number:

Reference to the run number of the entry: