System Assessment Report[1]

Relating to Electronic Records and Electronic Signatures;

21 CFR Part 11

System: StabNet
(Software Version 2.0)

---

[1] This report assumes that all system settings necessary for ERES compliance are set

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, e.g. conformity certificates, prepared documentation for IQ and OQ, carrying out IQ and OQ at the operator's premises.

Run no.	Ref.	Topic	Question	Yes	No	Comments
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 user id, date, time with difference to UTC (Coordinated Universal Time) and user. This time is taken from the client's system time, which means that the administrator has to take care of the system time to be correct, e.g. by synchronizing client with a reliable time server. In the report generator, the report can be defined in order to indicate any modified results data (results). Sample data modifications are recorded with the audit trail of the respective results. For method modifications all former versions are saved in the database and a comment has to be entered. Methods are subject to a version control. This means that modified data of a method leads to a new entry (version) in the database. If the results data are changed (recalculation), all former versions are saved in the database and a comment has to be entered. A version check is implemented for determinations. This means that modified data leads to a new entry in the database. Incomplete records of methods are identified by the fact that they cannot be saved. Invalid methods can be loaded but the associated analysis cannot be started. Invalid results can be recognized if limit values have been defined. In case of exceeding this limits it can be defined in the system whether a message is displayed on the screen or on the report or whether an email is sent. In the event of a corrupted database, the system tries to recover the respective database. If a corrupted database cannot be recovered, the system indicates this with a specific error code.

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		Method parameters can be printed out as part of a configurable report.
						Configurable reports can be printed out for 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 defined in the method. 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.
						To print out an old version of a method or determination, the respective record has to be changed to be current version.
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 can be stored as encrypted XML file (RDET format) and processed with StabNet.
						Data can be exported to XML, CSV, TXT and RDET format.
						Via the report generator all reports can be provided in PDF format.[2]
						The automatic data export 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 follow any alteration, overwriting or deletion of the data of a determination.

[2] Basically, the system allows to merge system-generated PDF files without entering a password - however, this option is available only if the 21 CFR Part 11 security settings are <u>not</u> enabled

Run no.	Ref.	Topic	Question	Yes	No	Comments
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. *StabNet* is installed with a local server. The system can permanently store the data either in the *StabNet* database or on the computer or on a network drive by using an archiving system or via paper print-out. The database has an automatic backup function, which automatically indicates whether a backup job was successful or not. The data on the storage device is encrypted and provided with a checksum. In this way it is protected against accidental and improper alterations. Alterations are recognized by the system. The content can be read by the *StabNet* software at any time. The method used for archiving data and which data are to be archived must be defined by the operator. Interfaces for archiving (XML files) are available 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 is provided with a login system with an unlimited number of editable profiles (access rights / user groups). The access rights for the single user groups can be arbitrarily defined by the administrator. The person responsible for the system must ensure that access rights are assigned to authorized persons only. All changes of access rights are recorded in the audit trail.
1.7	11.10 (e)	Audit Trail, Electronic Record, Operator Entries, Reason for Change/Deletion[3]	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?[3]	X		The audit trail documents all relevant user entries and actions on electronic records with user name, date, and time (with difference to UTC); changes to methods, determinations or sample data (only live modifications) require the entry of a comment by the user. Additionally, all modifications of security settings, user administration or configuration data are recorded in the audit trail.
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		A new version is automatically created, if methods or determination data are changed and saved.

---

[3] The reason for change or deletion is not originally a 21 CFR Part 11 requirement but reasonable for general GxP compliance and required by the EU Annex 11

Run no.	Ref.	Topic	Question	Yes	No	Comments
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		The data in the configuration database are kept as long as the audit trail has not been deleted. The disk space is the limiting factor here. The audit trail can only be deleted after it has been archived before. The audit trail is being archived as a text file with a checksum. If configured, the system requires a double check before the audit trail can be deleted; this double check is available to specific user rights only. The operator is solely responsible for the safe storage of the archived audit trail.
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 to a text file and is therefore available in electronic form. By means of the checksum, the data integrity of the audit trail can be verified. Additionally, a read-only PDF file of the audit trail can be created. If this PDF file is printed, the audit trail is also available on paper. The system is able to monitor the number of audit trail records in the database, in order to support the performance when the audit trail is read.
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 a database is assigned to the selected method, or whether the required device is available. The parameters of the determination are programmed in the method and must be strictly maintained.
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 must ensure that access rights are assigned 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 reviewer and the approver are not the same person. Additionally the rights assigned to a group can be restricted, so that their members are able to use signed methods only.

chemgineering

Ω Metrohm

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		During the IQ all the devices connected are entered into the list of instruments and are subsequently checked. Metrohm instruments are recognized, their validity is being checked and they are automatically entered into the list of devices. 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 training of the users 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 training on 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 that clarifies the equivalence of handwritten and electronic signature.
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 manual supporting the user and the service personnel. Additionally the content of the manual is available as Online Help. Distribution of paper-based system 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 system and a software version. Release notes are kept with each software version – except for the initial version 1.0. 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		StabNet 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 a modification the data become useless. Even if corrupted data are transferred to another system this is recognized.
2.2	11.30	Digital Signature	Are digital signatures used to authenticate the involved parties?	N/A		StabNet is not designed to be accessed via the Internet.

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 dropdown list) for signing. Additionally, a comment 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 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		Each user gets a unique login name, which is displayed together with the signature data. The system ensures that this login name is unique system-wide. Once a login name is created it cannot be deleted any more – it can only be deactivated. It must operationally be ensured, that user 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		The 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 the rights for electronic signing are assigned to this respective person?	O		With the assignment of the initial 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 credentials (user name and password) only for signing.
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		The data of the database are encoded in a format non-readable for humans. The administrator defines an initial password that has to be changed with the first login. The operator is responsible to control that a login name is handed over to the designated user only.

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		In StabNet electronic signatures are not 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 name) is used only once within the system and therefore each combination of identification code and password can also only exist once. Alterations of names must be managed by the operator. 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.
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. After this period is expired, the user is forced to change his/her password. The system saves the password history and therefore reusing 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 procedure has to be set up by the operator. The corresponding user 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 corresponding user 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.
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 generated, saying that the maximum number of unsuccessful login attempts has been reached and the user is disabled. A corresponding message can be sent to the management by email. All attempts to log-in to the system are recorded in the audit trail.
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 for informing the responsible management 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.

Legend

X   Applies to the system
O   Implementation in the operator's responsibility
N/A   Not applicable to the system

This 21 CFR Part 11 assessment is based on a physical audit of StabNet 1.0, performed March the 7th 2012. According to Metrohm AG (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 8.103.8025EN, and 8.0103.8005EN). Therefore, this update does not require a physical re-audit.

8 Indices

References to the page number:

References to the run number of the entry: