Endress+Hauser Advanced Data Manager Memograph M RSG45 Equipment evaluation within the requirements of Title 21, Code of Federal Regulations Part 11, latest revision (21 CFR Part 11)

Equipment:	Advanced Data Manager Memograph M RSG45
Manufacturer:	Endress+Hauser Wetzer GmbH+Co. KG, Germany
Computer system:	FDM Field Data Manager (PC software, MS-Windows® compatible)
Manufacturer:	Endress+Hauser Wetzer GmbH+Co. KG, Germany

Part 11 Section	System requirements	Comments
Subpart A – General Provisions		
§ 11.1	Scope.	
§ 11.2	Implementation.	
§ 11.3	Definitions.	
Subpart B – Electronic Records		
B § 11.10	**Controls for closed systems.**	
11.10(a)	Is the system validated to ensure accuracy, reliability, and consistent intended performance?	**Yes.** A MTBF value depending on the hardware configuration of the Advanced Data Manager is calculated according standard SN29500 and stated in the user manual. Whilst the SD-card/USB-stick is removed, the signals are still recorded via the internal memory. Warning is generated, if no SD-card/USB-stick is inserted afterwards. Warning is generated before the memory capacity is exceeded. Descriptive measures in the user manual about the secure usage of the external

Part 11 Section	System requirements	Comments
		storage medium. RS232 / Ethernet: Interruption of communication between the data manager and the PC gets detected (with alarm capabilities; audit trail logging in FDM). Automatic self-tests of the Advanced Data Manager (e.g. software program integrity via CRC at start-up and during run-time, Signal Input Range validation during run-time, Battery check during run-time, storage capacity check during run-time FDM Software: Any modification of external stored data in the FDM software is not possible, only an attachment of comments is allowed; the comment is marked as user comment. Audit Trail cannot be deactivated.
11.10(a)	▪ Is the system validated to ensure the ability to discern invalid or altered records? ▪ Does the system ‘flag’ invalid records? ▪ Does the audit trail track altered records?	**Yes.** All data (measured values and the audit trail) are stored in a special binary file format within the data manager – preventing user manipulation. FDM software accepts only data in the proprietary binary file format, which includes data integrity mechanism (CRC). This prevents data acceptance from invalid devices / data loggers. Numbering mechanism for each data packet prevents undetected loss of data packets (or incorrect sequence of data packets). Where it is possible to gain access to modify the records, the PC application would ‘flag’ the data as ‘not reliable’. The export of data in the “CSV” format (human readable) from the PC to other devices is supported. Displayed or printed records, stored in “.CSV” format, are automatically associated with a warning that they are not reliable.

Part 11 Section	System requirements	Comments
11.10(b)	▪ Is the system capable of producing accurate and complete copies of records in human readable and electronic format for inspection, review and copying by the regulatory agency? ▪ Can records be extracted in a format that can be read by the regulatory agency? ▪ Are annotations (e.g. “comments”) included as part of the record?	**Yes.** **Electronic format:** All data / information annotations / comments are stored in a proprietary binary file format and can be read / displayed direct at the unit in human readable form. The FDM software provides capabilities of converting the proprietary binary format of electronic records into the common human readable „.CSV“ or „PDF“ format. The (converted) electronic records contain complete data including audit trail and electronic signature information. All data (measured data, audit trail, electronic signature) are stored together in one file. **Human readable from:** Records can be printed at the PC using FDM. The printout contains the complete data (measured data, device name, date of file, audit trail, electronic signature information as requested by §11.50 b) The customer selects the desired information that is needed. The customer validates the printout by review and signature. The printout includes pagination information (sequential page numbering, each page refers to next page; the last page indicates the end of record.

Part 11 Section	System requirements	Comments
11.10(c)	Are the records protected to enable their accurate and ready retrieval throughout their retention period?	**Yes.** Data are automatically copied from the Advanced Data Manager’s buffered main memory to secondary (removable) storage memory if available. So either the removable SD-cards can be archived and / or data can be read out and stored on any other storage media (e.g. DVD, NAS drives…). Data is stored in a proprietary binary file format to protect against undetected corruption. The integrity of the records at the data manager is ensured via CRC. The CRC is part of the record file. The Advanced Data Manager is only intended for temporary storage of records (via internal memory and SD-card). For long term storage the records need to be transmitted to the PC using FDM. FDM enables automatic periodical read out and storage of the records. Data reviewed via the FDM software is protected and considered ‘tamper-proof’: Data can be de-coded and displayed but not changed / tampered via the FDM software.

Part 11 Section	System requirements	Comments
11.10(d)	▪ Is system access limited to authorized individuals? ▪ How are users authorized to get access? ▪ How is access modification and deletion managed? ▪ Is access periodically checked? ▪ Does the system provide adequate security? ▪ Do different access levels exist?	**Yes.** Both, FDM and the Advanced Data Manager provide the same methods to prevent unauthorized access i.e. multi-layered password protection in relation to the functional role of a person. The Advanced Data Manager has implemented a user administration (user/administrator with certain read and write rights and unique password/ID combinations). The device can be write-protected by activating a digital input configured for this purpose. In addition to this, access to the terminals on the rear side of the device can be physically protected with a hardware cover. Only the administrator can add new users using one unique ID or delete old users in the user administration. Deleting old users does not influence or change the recorded data / assignment of recorded data to the responsible user at that time. The password/ID combinations can be periodically renewed (forced by the unit, e. g. every 30 days). The password complexity can be configured. Only the Administrator has access to all levels of the setup configuration as well as responsibility for the creation, maintenance and deletion of other user level accessibility. Changes of device configuration will be documented in the audit trail. The other user levels have access only to specified operation of the Advanced Data Manager but not to the setup configuration. Neither the Administrator nor the Operator has access to manipulate the measured values or audit trail. It is allowed to add notations (comments) which are stored in the audit trail. This also requires entering the unique ID-/ password combination.

Part 11 Section	System requirements	Comments
		FDM Software: FDM has implemented a user administration (user/administrator with certain read and write rights). The password policy can be configured. The user administration has to be activated. The validity period of the password can be configured. At the first login, the password has to be changed. Connection to the database server is only possible with user authentication (ID / password). The communication settings in the application can only be changed by the administrator.

Part 11 Section	System requirements	Comments
11.10(e) (1)	▪ Is there a secure, computer generated, time stamped audit trail that independently records the date and time of operator entries and actions that create, modify or delete electronic records? ▪ Is the audit trail protected from intentional or accidental modification? ▪ Is the audit trail always activated? ▪ Is the audit trail computer generated? ▪ Is the date and time recorded? ▪ Is the time local to the activity? ▪ Is it protected from unauthorized change? ▪ Is time recorded to the second? ▪ Is the operator name captured? ▪ Does the audit trail track operator entries and actions that create, modify or delete records? ▪ Can the type of action be determined from the audit trail?	**Yes.** Automatic computer generated audit trail is implemented in the Advanced Data Manager including time stamp information; year-month-day; time (hh:mm:ss); operator action; operator identification. In addition to this all alarms, power downs, system messages, attempts to access the unit etc. are automatically stored in the audit trail. Records cannot be modified or deleted, except from adding notations or comments which are also stored in the audit trail. This is only possible after login using unique ID-/ password combination. FDM Software: Automatic computer generated audit trail is implemented inside FDM, including time stamp information; year-month-day; time (hh:mm:ss); operator action; operator identification. The audit trail information logs all operator entries and actions. FDM does not support capabilities to create and modify records. Audit trail is saved together with the measured data in one file in a special binary format inside the FDM database. The records are CRC protected.
11.10(e) (2)	Upon making a change to an electronic record, is previously recorded information still available (i.e. not obscured by the change)?	**Yes.** Records cannot be modified. It is possible to add notations or comments. Previously recorded information is available in data manager’s buffered main memory for a limited time period (programmable as first-in / first-out or stack memory). FDM users have not the capabilities to create or modify electronic records. Archived information is always available via the PC application FDM.

Part 11 Section	System requirements	Comments
11.10(e) (3)	Is an electronic record's audit trail retrievable throughout the record's retention period?	**Yes.** The entire audit trail is recorded to memory and can be viewed at any time using the PC application FDM. Recent audit trail 'entries' are available within the data manager's buffer memory and can be viewed by the user direct at the unit using easy to handle search functions.
11.10(e) (4)	▪ Is the audit trail available for review and copying by the FDA? ▪ Can the audit trail be printed? ▪ Can records be extracted in an electronic format that can be read by FDA?	**Yes.** The audit trail is stored and can be read / displayed direct at the unit in human readable form. Using PC software FDM the audit trail – like every recorded information – can be inspected / reviewed, archived, copied, and also displayed and printed in human readable form (e. g. for FDA reviews). PC software FDM is allowed to be used wherever it is needed.
11.10(f)	If the sequence of system steps or events is important, is this enforced by the system (e.g. data must be entered before it can be approved)?	**Yes.** The Advanced Data Manager and FDM do not allow entering data / commands before the user has successfully logged-in. Operational system checks: Guidance for the operator via a menu driven user interface at RSG45 and FDM. Only authorized users are allowed to make signatures on the records.

Part 11 Section	System requirements	Comments
11.10(g)	▪ Are there checks in place to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand? ▪ How are users authorized to get access? ▪ How is access modification and deletion managed? ▪ Is access periodically checked? ▪ Does the system ensure adequate security? ▪ Do different access levels exist? Are they documented? Are they enforced by the system?	**Yes.** The Advanced Data Manager and FDM providing a multi-layer authorization model (e.g. administrator, main user, user level, user level 2, user level 3). The “main user”, “user level”, “user level 2”, “user level 3” for the RSG45 and “Planning Engineer”, “Service Engineer”, “Maintenance Engineer”, “System Engineer” and “Observer” for FDM are hereafter called “Operator”. System access and modification are allowed only by person(s) with ‘Administrator’ rights: only the administrator can add new users using one unique ID or delete old users in the user administration. Deleting old users does not influence or change the recorded data / assignment of recorded data to the responsible user at that time. Records cannot be altered – only appended (e.g. the addition of notations and comments). Access requires an electronic signature consisting of a unique ID / Password combination. The unit may force users to renew their password e. g every 30 days. User is denied after multiple incorrect user / password entries. Inactivity function requires new entry of user name and password after a certain time.

Part 11 Section	System requirements	Comments
11.10(h)	If it is a requirement of the system that input data or instructions can only come from certain input devices, does the system check the validity of the source of data input or operational instructions?	**Yes.** The Advanced Data Manager must be set up correctly, including terminal connections, to properly record the incoming electrical signal(s). The terminals for connecting sensors have a metal hardcover protection, it can be sealed, so a removal of the protection cover or sealing is obviously manually detectable. FDM software: Validity of data input is checked by CRCs, assignment of data base to device serial number and transaction handling. A session handling is implemented. A device configuration via FDM is not possible.
11.10(i)	Has it been determined and properly documented that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks?	**Yes.** The development team for the Advanced Data Manager and PC application FDM has been properly and professionally trained in 21 CFR 11 requirements. The manufacturer is certified according to ISO 9001. (Training of the persons who maintain or use the systems is the responsibility of the user / company.)
11.10(j)	Are there written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification?	**N/A.** (This is typically the responsibility of the user / company.) As an additional help the Advanced Data Manager displays a message to the user indicating that this act is legally binding and equivalent to a handwritten signature when entering his electronic signature.
11.10(k)(1)	Do adequate controls exist over the documentation for the distribution of, access to, and use of systems operation and maintenance documentation controlled?	**N/A.** (This is the responsibility of the user / company.)

Part 11 Section	**System requirements**	**Comments**
11.10(k)(2)	Do revision and control procedures exist to maintain an audit trail that documents time-sequenced development and modification of systems documentation?	**N/A.** (Maintenance of documentation copies is the responsibility of the user / company).
B § 11.30	**Controls for open systems.**	
11.30	▪ Do procedures and controls exist, as necessary in an open system, to ensure record authenticity, integrity, and confidentiality from the point of record creation to the point of receipt? ▪ Is document encryption used? ▪ Are digital signature standards used? ▪ Are other controls required?	**N/A.** (The Advanced Data Manager / FDM is a closed system. The access to it / the recorded data is controlled only by persons who are allowed to handle the unit or who are responsible for the contents of the recorded data.)
B § 11.50	**Signature manifestations.**	
11.50(a)	Do signed electronic records contain information associated with the signing that clearly indicate: 1. The printed name of the signer; 2. The date and time when the signature was executed; 3. The meaning of the signing associated with the signature; ▪ Are date and time applied by the data manager? ▪ Is the time local to the signing? ▪ Is the time protected from unauthorized change? ▪ Is time recorded to the second?	**Yes.** Recorded data are automatically assigned to the responsible user identified by his electronic signature and can be reviewed either direct at the unit or using the PC software FDM. The signature contains user ID, his printed name and date / time (automatically generated by the unit) when the signature was executed. Time is recorded to the second and can only be adjusted during the unit setup or clock synchronization via FDM by the administrator.
11.50(b)	Are items 1, 2 and 3 above subject to the same controls as for electronic records and included as part of any human readable form of the electronic record?	**Yes.** Recorded data are automatically assigned to the responsible user identified by his electronic signature and can be reviewed in human readable format either direct at the unit or using the PC software FDM.

Part 11 Section	**System requirements**	**Comments**
B § 11.70	**Signature/record linking.**	
11.70	▪ Are electronic signatures and handwritten signatures executed to electronic records linked to their respective electronic records to ensure that the signature cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means? ▪ How is the record and signature linked? ▪ Is the signature protected to prevent transfer to another record? ▪ Is the signed record protected to prevent changes after signing? ▪ If the record is changed, is the signer prompted to re-sign following the change?	**Yes.** Electronic signatures are saved together with all data in one record file. This ensures unique linkage between electronic record and electronic signature. The Advanced Data Manager is always recording measured values based upon the incoming electronic signal. To designate a production run or batch (that consequently activates the control functions of the Advanced Data Manager), an authorized user must first sign in with his/her electronic signature. This person's name is subsequently linked to all data (measured values and audit trail events) until the person executes his/her closing signature or until the next authorized user signs in. Records and signatures are permanent. They can´t be changed by ordinary means. It is not possible to remove electronic signatures from the affiliated electronic data.
Subpart C – Electronic Signatures		
C § 11.100	**General requirements.**	
11.100(a)	▪ Is each electronic signature unique to one individual? ▪ Is an electronic signature ever reused by or reassigned to anyone else?	**Yes.** Each electronic signature is unique to one individual using a unique ID / Password combination. The creation and presence of two identical user IDs is technical prevented. Changing the password requires a new password that hasn't been used for a reasonable time. The Advanced Data Manager maintains a list of active signatures. (Assignment and/or selection of unique IDs are the responsibility of the administrator.)

Part 11 Section	System requirements	Comments
11.100(b)	Is the identity of an individual verified before establishing, assigning, certifying or otherwise sanctioning an individual's electronic signature, or any element of such electronic signature?	**N/A.** (This is the responsibility of the user / company. To assist an initial password is provided by the administrator which has to be changed by the user before he/she can do anything with the instrument.)
11.100(c)	Has the user notified the regulatory agency that the electronic signatures in its system are intended to be the legally binding equivalent of traditional handwritten signatures?	**N/A.** (This is the responsibility of the user / company which have to inform the Office of Regional Operations (HFC100), 5600 Fishers Lane, Rockville, MD 20857, on a traditional letter with handwritten signature that the company intends to use electronic records / electronic signatures in future.)
11.100(c)	▪ If electronic signatures are being used, can additional certification or testimony be provided that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature? ▪ Is there any documentation to support that individuals understand that electronic signatures are the legally binding equivalent of their handwritten signatures?	**N/A.** (This is the responsibility of the user / company. To assist this the Advanced Data Manager displays a message indicating that this act is legally binding and equivalent to a handwritten signature when entering his password at the unit.)
C § 11.200	**Electronic signature components and controls.**	
11.200(a)(1)	Is the non-biometric signature made up of at least two (2) distinct identification components, such as an identification code and password?	**Yes.** The electronic signature consists of one unique identification code (ID) and one password. The unique ID and one initial password are defined by the administrator. A user can only operate the instrument after changing the initial password to one which is only known by him. Each ID / Password combination must be unique.

Part 11 Section	System requirements	Comments
11.200(a)(1)(i)	▪ When an individual executes a series of signings during a single, continuous period of controlled system access, is the first signing executed using all electronic signature components, and subsequent signings are executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual? ▪ Are both electronic signature components required for the first signing? ▪ Is the period of continuous use defined? ▪ Does the system log off after a period of inactivity? ▪ If only one component is required (as in subsequent signings), is it the private component?	**Yes.** Prior to initiating a production session, someone ('Administrator' or 'Operator') must be designated as the person of record (...person with responsibility for the production session.) The system is logged automatically after a specified amount of time if the automatic logout is activated. If the automatic logout is deactivated, the system does not log till the user logs off or another user may assume the session responsibility by logging in with his/her unique ID / Password combination. For each operation, which requires user identification, at least the private component (password) has to be entered.
11.200(a)(1)(ii)	When an individual executes one or more signings not performed during a single, continuous period of controlled system access, is each signing executed using all of the electronic signature components?	**Yes.** User has to enter his/her complete electronic signature (unique ID-/ Password combination).
11.200(a)(2)	▪ Are non-biometric signatures used only by their genuine owners? ▪ Are there procedures and training to reinforce that non-biometric electronic signatures are to be used only by their genuine owners (not shared, not loaned, not borrowed, not posted)?	**N/A.** (This is the responsibility of the company which should train the users how to handle the electronic signature. To assist this the Advanced Data Manager displays a message indicating that this act is legally binding and equivalent to a handwritten signature when entering his password at the unit.)

Part 11 Section	System requirements	Comments
11.200(a)(3)	▪ Are non-biometric signatures 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? ▪ Could one person working alone "forge" another person's electronic signature?	**Yes.** The electronic signatures are unique for each user / administrator. Different password length may be set for administrator and users (up to 12 characters). They are stored in special binary format. Using an appropriate password length ensures that it is not possible for one or more persons to forge another's electronic signature. Attempted and failed execution of electronic signatures is automatically recorded in the audit trail.
11.200(b)	Are electronic signatures based upon biometrics designed to ensure that they cannot be used by anyone other than their genuine owners?	**N/A.** The Advanced Data Manager does not incorporate the use of biometric based electronic signatures.
C § 11.300	**Controls for identification codes/passwords.**	
11.300(a)	▪ Are controls in place to maintain the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password? ▪ Is uniqueness ensured historically as well as currently? ▪ Does the process of assigning accounts ensure uniqueness? ▪ Does the system prevent re-use of usernames?	**Yes.** The administrator has to ensure unique IDs / user names. The Advanced Data Manager does ensure that all active, authorized electronic signatures are unique. (Unique identification code and the use of initial passwords are the responsibility of the administrator.)

Part 11 Section	System requirements	Comments
11.300(b)	▪ Is the issuance of identification codes and passwords periodically checked, recalled, or revised (e.g. to cover such events such as password aging)? ▪ Do passwords periodically expire and need to be revised? ▪ Is there a procedure for recalling identification codes and passwords if a person leaves or is transferred?	**Yes.** The Advanced Data Manager can be set up to monitor password aging or expirations. If used the user has to renew his/her password in a specified cycle (e. g. each 30 days). Person(s) with 'Administrator' rights has (have) the authority to add/delete the ID and password for authorized users. Passwords cannot be recalled but in each case historical data can be assigned to the responsible user at that time.
11.300(c)	Are there 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?	**N/A.** Tokens, cards, or other devices which bear or generate identification code or password information are not used. (This is the responsibility of the user. To assist this, the administrator can delete existing users, e. g. if unauthorized attempt is detected / recorded in the audit trail).
11.300(d)	▪ Are there 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? ▪ Does the system prevent unauthorized access? ▪ Are break-in attempts monitored?	**Yes.** The Advanced Data Manager and PC software FDM prevent unauthorized access. Limitation of incorrect system log-in attempts is provided. When the limit is exceeded, the user access is denied. The Advanced Data Manager will store break-in attempts in the audit trail. (Additional or other transaction safeguards are the responsibility of the user / company.)
11.300(e)	Are there procedures covering the initial and periodic testing of devices, 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?	**N/A.** Tokens or cards, which bear or generate identification code or password information, are not used.