La Spezia, 03/08/2022

21 CFR Part 11 checklist

The evidence, results and any findings found with respect to 21 CFR 11 are listed below. The software MIG version 7.10 is a storage and management system of the maintenance plans. In the database there are stored the technical data sheets of the equipment / systems, warehouse movements (spare parts), management of the people authorized to carry out maintenance and operations on MIG.

By "equipment / systems" means everything that is a "structural element" subject to periodic or corrective intervention (ISO 10147). It therefore also includes measurement and control instrumentation.

Sec. 11.10 Controls for closed systems	
Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:	LOGIN: Failure to login test if username or assword are wrong is performed. An alert message appears.
	The password policy is verified: the password must be changed on a period that can be set by the administrator from 1 day up to 365. - The renewal of the password excludes to reintroduce the old password. A negative test issued an error message. - The username can be blocked after X failed access for each username or each IP address. The blocking system blocks the failed login in a period of Y minutes. X and Y are set by the administrator. - A log of the failed access is permanently recorded.
	Verified that the login with a barcode or QR code requires also the password.
	Verified the log file where of each operation has been recorded as new or changed with the MIG username, the windows username, and the operation performed. For the changes the old and new data are recorded. The authenticity of the author of the record introduced or changed is granted and cannot be repudiated because the log data cannot be change by any person (including the administrator).
	MIG has adopted the login system allows to introduce: Username, badge, systems provided by the customer for the identification of personnel, Password entered manually
	The login determines the access priorities to the software modules with: • Read / write access • Read-only access • Cancel access • Access denied

	• Limits of accessible records/areas.
(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Verified: • Instruction manual include also the installation procedure with many tasks that verify the correct installation. See section “Installazione Applicazione MIG” of the Italian IFU as wella s section “MIG INSTALLATION” in the English version. Refer to “User Manual v.7.6.2”. • Form VerbControllo rev. 2 date 13/06/2022 as installation records. Both documents assure the validation of each installation towards accuracy, reliability, and performance through several actions and verifications.
(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.	The MIG software can perform printouts of the information on layouts that can be defined by the administrator. The data printed cannot be modified prior the printout. When the output device is set as printer, the data is reliable for FDA inspection. All other devices include PDF, XLSX, DOCX, PPTX, RTF, etc, can be modified after the relevant file generation.
(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	The database is unique and corresponds to a single area which is the working area. From here, any data can be recovered to be read without any retention time limit. The backup scheduling function is provided by MIG including the time frame, the destination of the backup, the verification of the correct backup, a message to the IT manager in case of failed backups. MS SQL Server database is Database Management System with versions from standard up to enterprise depending on the choice of the client.
(d) Limiting system access to authorized individuals.	See introductory part concerning the login system.
(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	Verified that the log file registers the date and time the operation is performed by the software independently when the operator creates, or modify or delete the electronic records. There are another fields related to date and time filled by the operator, but the log is not affected on the registration date and time.
	The records can be deleted after a number of years defined by the administrator from 2 year up to no limits (21 CFR 820.180.(b)). The default value is 10 years.
	The log file records don’t have a time limit.
	There is also a checksum in each record to assure that even if a data corruption is performed on the database with an access mean different from MIG, the corruption is detected with a “verify” function.

(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	The maintenance statuses are: • request [extraordinary] / planned [ordinary] • confirmation / defined scheduling (mandatory) • opening of the intervention • operational / economic final report – data statement • closure (mandatory) • cancel the maintenance (alternative to closure) • suspension of the maintenance (alternative to closure)
g) Use of authority checks 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.	Access to the MIG system is through user profiles and groups that establish access rights. Access to the system is in the hands of the MIG administrator. The accesses establish for each element whether or not it is accessed and whether it is accessed, in read only, or in writing and reading
(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	See introductory part concerning the login system.
(i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	Verified the Instruction for use Manual rev.: 7.6.2 where a complete explanation of the software system allows the system manager to perform all setups. TAM SOFTWARE provide al least a 4 hours training for the system manager and maintenance people. Verified the offer n° 22/0083 I 2022/07/11 where a training of 8 hours is offered.
(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	The policy is the responsibility of the customer, but the VerCollaudo rev.2 installation test report shows the main policy elements of the actions that guarantee the truthfulness of the information and methods to avoid data and signatures falsification.
(k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.	The System documentation supplied is a user manual (Verified rev.7.6.2 and release note 7.9.3). It includes both information for the operating user and for the System Manager. The manual is released upon installation.
(2) Revision and change control procedures to maintain an audit trail that documents time- sequenced development and modification of systems documentation.	Upon updating, the release notes are transmitted in all clients systems and the notification of the change and its impact on the operator / system manager is sent via email. The change documentation with start and validation dates is managed inside TAM. Verified: the request for modification of RdM 2015.01_RM92 of 22/03/22; on revision 7.9.3, filed in the Azure DevOps versioning system which includes any changes to the IFU in the notes

	field if there are any.

Sec. 11.30 Controls for open systems.	
Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	NA

Sec. 11.50 Signature manifestations.	
(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of thefollowing: (1) The printed name of thesigner; (2) The date and time when thesignature was executed; and (3) The meaning (such as review,approval, responsibility, orauthorship) associated with the signature.	The signature takes place with the status transition of the maintenance process based on the username of the person carrying out this step. The actions on the process phase are signed when the MIG system requires the signature that identifies the person The system manager determines which stages can require mandatory signing. Verified: The signer's name appears Verified: The date and time of registration appears Verified: The meanings of the record are : • request [extraordinary] / planned [ordinary] • confirmation / defined scheduling (mandatory) • opening of the intervention • operational / economic final report – data statement • closure (mandatory) • cancel the maintenance (alternative to closure) • suspension of the maintenance (alternative to closure)
(b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).	Verified: an example of a complete process including the main phases of the maintenance steps. All steps are clearly visible on the display of the record as well as they are visible in a paper printout. The printouts can be modified by the system manager to include the information needed to perform a control or audit of the

	maintenance process.

Sec. 11.70 Signature/record linking.	
Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.	NA

Sec. 11.100 General requirements.	
(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	The uniqueness of the signature is managed by the customer. The signature consists of the combination of "Username" + "Password". The homonymy of the username is not possible and it is detected by the system MIG.
(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.	Verified: the system MIG allows to perform two levels of the signature control: • The LOG registrations in order to track all changes performed on each record (the changes are linked to the individual) • The checksum to detect any data corruption (without individual detection if no transection Log on SQL server is not activated). Through the backup it is possible to retrieve the original data.
(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures. (1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857. (2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.	Verified: • The account creation process requires to the individual to accept that the electronic signature is equivalent to a handwritten one. • In the Form VerbControllo rev.2 the mandatory signature policy related to the electronic signature is clearly stated and transferred to the client's system manager, in order to assure that a form with the certification of equivalence of the electronic signature to the handwritten one is approved and signed by each individual.

Sec. 11.200 Electronic signature components and controls.	
(a) Electronic signatures that are not based upon biometrics shall:	
(1) Employ at least two distinct identification components such as an identification code and password.	The login is based upon a USERID and a PSW
(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.	Verified: two successive registrations. The first one requires both username and password. The second one requires the password only
(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.	See the previous requirement. The system performs a automatic logout after a time frame from 1 up to 60 minutes. The time frame can be set by the system manager. After the automatic logout a double login information is required.
(2) Be used only by their genuine owners; and	The policy transferred by TAM SOFETWARE to the client is to avoid to disclose the login information to third parties for every individual. The MIG forces to change periodically the password in order to avoid that mis-login can be maintained for long time.
(3) Be 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.	USERNAME e PASSWORD along with the User's policy can assure that non attempt to a false signature can be done without the collaboration of the original individual
(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners	NA

Sec. 11.300 Controls for identification codes/passwords	
Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include	Verified: no Homonymy is possible with the same username.
(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.	Verified: the password validity has time limit as already above described.
(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	Verified
(c) Following loss management procedures to	Verified: The Form VerbControllo rev.2 states in

electronically deauthorize 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.	the policy transferred to the client that in cases of lost, missing or stolen badge or other device to inform the emitting office to adopt the adequate actions.
(d) Use of 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.	Verified: The MIG system allows each user to have only one open session at a time. In the presence of an intrusion by an unauthorized person, a message is sent to the original user with the address of the PC where the session in running, in order to inform the system manager of the intrusion.
e) 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.	Verified: The Form VerbControllo rev.2 states in the policy transferred to the client that the Badge system must be verified every 6 months at least.