21 CFR Part 11
Compliance Assessment Report

No. Doc.10.2402

Product Name:	Delta DIAView SCADA System
Version:	4.1.0
Appraiser:	ALLY ZHOU
Report Date:	2024.02.04

21CFR Part 11	Details	Applicable	Meet Requirements	Note/Suggestion
§ 11.10	**Controls for closed systems**			
§ 11.10	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.	YES	YES	DIAView SCADA System has taken steps to ensure that access to the system is granted only to designated personnel and that data is stored in a dedicated format to provide a high level of security. There is no means available to modify the saved data. Electronic signatures made using DIAView SCADA System cannot be removed. Controlled user permissions prevent users from using anyone else's electronic signature other than their own.
§ 11.10 (a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	NO	/	DIAView SCADA System is a software which can help users to develop the application they would like to create. Meanwhile, as for audit trail, DIAView has the ability to discern invalid data, there is a special column for users to check whether this data is invalid or not. Once the records are altered or changed, this value will mark “invalid”
§ 11.10 (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.	YES	YES	DIAView SCADA System generates electronic files in a software-readable format that can be accessed and read. Or print the data for people to read. These files can be easily copied for backup, archive, review, and review purposes.
§ 11.10 (c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	YES	YES	DIAView SCADA System generates electronic files in a software-readable format that can be archived for long-term storage and retrieval, or the files can be copied or exported to other long-term archiving media such as a USB flash drive or SD card.

21CFR Part 11	Details	Applicable	Meet Requirements	Note/Suggestion
				The user is responsible for the preservation and archiving of such data.

21CFR Part 11	Details	Applicable	Meet Requirements	Note/Suggestion
§11.10 (d)	Limiting system access to authorized individuals.	YES	YES	Supports the use of a combination of username and password to authorize individual access. Allows multiple users to register, and assigns different permissions to administrators and regular users as needed.
§ 11.10 (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.	YES	YES	DIAView SCADA System software creates a time-stamped audit trail to keep a record of all operational actions, including system startup, start of data logging, record generation, record modification, error messages (including unauthorized attempts to access), and record deletion. The system does not allow any user to modify electronic records that have been generated. The records of the audit trail cannot be changed by users or administrators. Each log created by DIAView SCADA System software is stored in a set database and can be copied for long-term storage along with associated data files. The specific storage time and method are determined and managed by DIAView SCADA System user.
§ 11.10 (f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	YES	YES	DIAView SCADA System Software system logs and data records are arranged by time.
11.10 (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.	YES	YES	DIAView SCADA System software supports the use of a combination of username and password to authorize an individual's access. DIAView SCADA System has the function of electronic signature, that is, after the user enters the correct user name and password,

21CFR Part 11	Details	Applicable	Meet Requirements	Note/Suggestion
				his signature will be added to the software system record. Only administrators can create and delete users. Password validity period can be set. After the validity period expires, you must change the password to log in to the system. The same authorization check is performed when an electronic signature is attached.

21CFR Part 11	Details	Applicable	Meet Requirements	Note/Suggestion
§ 11.10 (h)	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	YES	YES	DIAView SCADA System software implements its functions as a closed system that can be configured in a local user interface. DIAView SCADA System can only be operated by authorized persons to identify the operator. DIAView SCADA System software can request double review of data and operations according to the setting requirements, and its operations will be recorded by DIAView SCADA System software and recorded in the audit trail, which can achieve traceability.
§ 11.10 (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.	NO	/	Training records and recognition of user qualifications are the responsibility of the company. The operating manuals provided by Delta Electronics Industries Limited can be integrated into the company's own training procedures.
§ 11.10 (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.	NO	/	It is the responsibility of the company to propose documented procedures to hold holders accountable for acts corresponding to their electronic signatures. DIAView SCADA System provides a secure electronic signature option to work with a company's internal procedures to help companies comply with regulatory requirements.
§ 11.10 (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. （2）Revision and change control procedures to	NO	/	Document preparation and monitoring procedures are established by each company according to its own situation.

21CFR Part 11	Details	Applicable	Meet Requirements	Note/Suggestion
	maintain an audit trail that documents time sequenced development and modification of systems documentation.			

21CFR Part 11	Details	Applicable	Meet Requirements	Note/Suggestion
§ 11.30	**Controls for open systems**			
§ 11.30	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.	NO	/	DIAView SCADA System is designed as a closed system. Access to records is controlled by the same person responsible for the contents of those records.
§ 11.50	Signature manifestations			
§ 11.50	(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: （1）The printed name of the signer. （2）The date and time when the signature was executed. （3）The meaning (such as review, approval, responsibility, or authorship) associated with the signature. (b) The items identified in paragraphs	YES	YES	When a record is signed, the user name, date, and time of signature are automatically recorded. The actions performed by the user are also recorded synchronously for traceability. These records cannot be deleted. All information related to an electronic signature can be reviewed by DIAView SCADA System software or presented electronically or printed for review.

21CFR Part 11	Details	Applicable	Meet Requirements	Note/Suggestion
	(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).			

21CFR Part 11	Details	Applicable	Meet Requirements	Note/Suggestion
§ 11.70	**Signature/record linking**			
§ 11.70	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.	YES	YES	Each electronic signature is linked to the relevant data set. Multiple electronic signatures can be applied to each record. Because the signature is permanently associated with the data file and stored in a dedicated format, it is impossible for any electronic signature to be deleted or copied.
§ 11.100	**General requirements**			
§ 11.100 (a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	YES	YES	DIAView SCADA System uses a combination of user names and passwords to authorize the system and manage the application of electronic signatures. Use the same level of permission as for entry to the system to manage the application of electronic signatures. An electronic signature is always based on a unique combination of username and password.
§ 11.100 (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.	NO	/	These controls must be implemented by the company using DIAView SCADA System software.
§ 11.100 (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, 1 997, are intended to be the legally binding equivalent of traditional handwritten	NO	/	This certification must be submitted to the FDA by the company using DIAView SCADA System software.

21CFR Part 11	Details	Applicable	Meet Requirements	Note/Suggestion
	signatures.			
§11.100 (c)(1)	The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations **(HFC-1 00), 5600 Fishers Lane, Rockville, MD 20857**.	NO	/	This certification must be submitted to the FDA by the company using DIAView SCADA System software.
§11.100 (c)(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.	NO	/	This certification must be submitted to the FDA by the company using DIAView SCADA System software.
§ 11.200	**Electronic signature components and controls**			
§ 11.200	（1）Employ at least two distinct identification components such as an identification code and password. （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. （ii）When an individual executes one or more signings not performed during a single, continuous	YES	YES	DIAView SCADA System supports a combination of two identification components to authorize access to the system, using a combination of both username and password. Each combination must be unique. Only one record can be signed at a time. Each signature requires each component of the electronic signature to be entered manually by the user. DIAView SCADA System requires a user name and password for each signature.

21CFR Part 11	Details	Applicable	Meet Requirements	Note/Suggestion
	period of controlled system access, each signing shall be executed using all of the electronic signature components.			
§ 11.200	（2）Be used only by their genuine owners. （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.	YES	YES	DIAView SCADA System passwords and user names cannot be viewed by other users. Passwords are stored in an encrypted format and cannot be viewed by the administrator. They can only be reset. The original default is a default expired password that the user must change before doing anything after the initial login.
	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	YES	YES	DIAView SCADA System uses a combination of passwords and user identities, as well as electronic signatures based on facial recognition technology.
§ 11.300	**Controls for identification codes/passwords**			
§ 11.300	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: (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. (b) Ensuring that identification code and password issuances are periodically checked,	YES	YES	DIAView SCADA System does not allow the combination of user name and password to be repeated. DIAView SCADA System password has a validity period. When the time limit expires, you must change the password and log in to the system with the new password. Companies using DIAView SCADA System software should establish processes to control this.

21CFR Part 11	Details	Applicable	Meet Requirements	Note/Suggestion
	recalled, or revised (e.g., to cover such events as password aging).			
§ 11.300	Following loss management procedures to 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.	YES	YES	DIAView SCADA System system log records all actions, and administrators can delete existing users if unauthorized attempts are detected. Documented procedures need to include specific controls for the maintenance, release, testing and tracking of assigned identifiers and passwords, with requirements set and implemented by the enterprise of the company using DIAView SCADA System. Tokens and cards are not used.
§ 11.300	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.	YES	YES	When DIAView SCADA System detects incorrect attempts to apply an electronic signature to a file that occur a specified number of times (usually 5), user access is automatically disabled. The operation is recorded in the system log. If the login is successful, DIAView SCADA System detects an incorrect attempt to apply an electronic signature to a file, prompts an error, and locks the user after the specified number of times.
§ 11.300	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.	NO	/	This certification must be submitted to the FDA by the company using DIAView SCADA System software.