MCT4_MCTB

21 CFR Part 11 Compliance and Technical Controls for 1/4DIN and "Slim-Line" Multi-Loop Controller.

Overview

21 CFR Part 11 requirements are part of the fundamental building blocks that make-up the MCT4_MCTB controllers. 21 CFR Part 11 Technical Controls may be enabled or disabled for the MCT4_MCTB. Once enabled, the following subparts are addressed by the control system:

Subpart	Topic	MCT4_MCTB Compliance
11.10 (a)	System Validation	√
11.10 (b)	Accurate and complete copies of records	√
11.10 (c)	Protection of records	√
11.10 (d)	Limiting system access	√
11.10 (e)	Computer generated audit trail	√
11.10 (f)	Operational system checks	√
11.10 (g)	Authority checks	√
11.10 (h)	Device checks	SOP
11.10 (i)	Education and training of personnel	SOP
11.10 (j)	Personnel accountability	SOP
11.10 (k)	Control of documentation	SOP
11.30	Controls for open systems	N/A
11.50 (a)	Electronic signature contents	√
11.70	Electronic signature lining to records	√
11.100 (a)	Unique electronic signatures	√
11.100 (b)	Identify verification	SOP
11.100 (c)	Certification of electronic signatures	SOP
11.200 (a)	Electronic signature components	√
11.200 (b)	Biometric electronic signatures	N/A
11.300 (a)	Unique IDs and passwords	√
11.300 (b)	Password aging	√
11.300 (c)	Loss Management	SOP
11.300 (d)	Transaction safeguards	√
11.300 (e)	Testing of biometric devices	N/A

Compliance Legend

√ = *Compliant when configured per the provided User Manual*
SOP = Must be addressed through customer's standard operating procedures
N/A = Does not apply

Compliance Details

THE MCT4_MCTB has been 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. In the requirements below, underlined content indicates the section of the clause specifically addressed by the MCT4_MCTB software.

21 CFR Part 11 Requirement	MCT4_MCTB Capability
Subpart B, Section 11.10 (a). "Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records."	• Completed data files by are closed by the system and permanently linked to an encrypted signature file • Additional encrypted digital signatures can be added to any closed data file if user has appropriate security rights • System checks integrity of closed data files – any change to a closed data file results in an integrity failure notification • View digital signatures for any file • Check integrity of file, digital signatures, and provide real-time results. • Validate systems using the OEM provided IQ/OQ documents
Subpart B, section 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."	• Automatically data log process parameters via secure, digitally signed data files • View the data log history • Export encrypted data for viewing on a personal computer using the Data Viewer. Data files cannot be altered by Data Viewer. • Data can also be converted to Excel spreadsheets for FDA inspection without altering the original data file. • Data files that have been altered will fail digital signature validation at the MCT4_MCTB and PC Data Viewer.
Subpart B, section 11.10 (c). "Protection of records to enable their accurate and ready retrieval throughout the records retention period"	• Provides ability to export all data records to USB Flash Memory/FTP/Cloud for transport to a personal computer (PC) • Once on the PC, data can be transferred to longer lasting storage media. Media can be labeled appropriately • Provides personal computer application that validates file integrity and allows viewing without altering the original data file • If secure files are modified in any way, the integrity is lost and the digital signature will fail.

21 CFR Part 11 Requirement	MCT4_MCTB Capability
Subpart B, section 11.10 (d). "Limiting system access to authorized individuals."	• Select the "type", or level, for a user and assign a unique username and password for each user. • Assign user rights, or privileges, for each user type • Optionally enable re-authentication to enforce security even if a user forgets to log-off. Re-authentication prompts the user for their username and password before changing any process control variable
Subpart B, section 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 for at least as long as that required for the subject electronic records and shall be available for agency review and copying."	• Continuously generate a detailed audit trail that includes time/date stamps of operator access, operator actions, system changes, setup changes, and other critical functions • The audit trail is an integral part of the electronic archive record and remains as long as the records are retained • The audit trail is viewable on the MCT4_MCTB display
Subpart B, section 11.10 (f). "Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate."	• Configurable user rights/multi-security level based enforcement with re-authentication option provides dual check of operator authentication before process changes can be made at the system level. • All operator actions recorded in a secure encrypted audit trail.
Subpart B, section 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."	• Each user is assigned to a one of four user groups or types. Each of the four groups can represent a different level of privileges and security • Permissions for each user group can be individually enabled and disabled for every major function of the system. • Optionally enable re-authentication to enforce security even if a user forgets to log-off. Re-authentication prompts the user for their username and password before changing any process parameter • All operator actions are recorded in a secure audit trail file • Checksums are used to verify the integrity of the files

21 CFR Part 11 Requirement	MCT4_MCTB Capability
Subpart B, section 11.50. Signature manifestations. "Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:" "The printed name of the signer;" "The date and time when the signature was executed; and" "The meaning (such as review, approval, responsibility, or authorship) associated with the signature." "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)."	• Secure, encrypted digital signatures can be added to completed (closed) data files • Signature data includes Date, Time, UserName, and User Comment (approved, closed, etc.) • Only users with the appropriate security rights can digitally sign a closed data file.
Subpart B, section 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."	• Digital signature file are automatically linked to each data file when the file is completed. • Any data file with a missing signature file will automatically fail during viewing at the MCT4_MCTB or provided PC data viewer. • Any attempt to re-link or match a signature file to data file other than its original will fail the digital signature inspection process. All encrypted, digital signature files are mathematically linked to the original data file for secure, tamperproof operation.
Subpart C-Electronic Signatures Subpart C, section 11.100 (a).General requirements "Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else."	• Digital signatures can be added by users with appropriate security rights only. This ensures the uniqueness of the individual signing the file. Once a user is authenticated by the system, the digital signature information is stored in an encrypted format. • Any attempt to modify or change the digital signature data will result in failure during the digital signature inspection process. • Any attempt to re-link or match a signature file to data file other than its original, will fail the digital signature inspection process. All encrypted, digital signature files are mathematically linked to the original data file for secure, tamperproof operation.

21 CFR Part 11 Requirement	MCT4_MCTB Capability
Subpart C, section 11.200. Electronic signature components and controls. "Electronic signatures that are not based upon biometrics shall: "Employ at least two distinct identification components such as an identification code and password." "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 use 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." "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." "Be used only with their genuine owners: and" "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. "Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners."	• Data entry for user login requires a unique UserID and password for all login operations • Only 3 attempts are permitted for user login, when the user login data does not match an authorized user in the system. • All successful and failed login attempts are written to the secure, encrypted audit trail. • The re-authentication option requires that all users must log in each time a system process change is made, even if the user is already logged in. • All login operation (and re-authentication login) requires the unique UserID and password during each login.
Subpart C, section 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:" "Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password." "Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging)." "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." "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 the unauthorized use to the system security unit, and, as appropriate, to organizational management." "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."	• Users of MCT4_MCTB system must employ controls to ensure the security and integrity of users and user data entered into the MCT4_MCTB system. • System can be configured to password expiration based on a configurable number of days. A new password will then be required, having provided the old one, before accessing any other functions. • Only 3 attempts are permitted for user login, when the user login data does not match an authorized user in the system. • The MCT4_MCTB system will not allow more than one user with the same UserID to be entered into the system. Each user entered into the MCT4_MCTB system must have a unique UserID. The administrator will be prompted during user entry if the UserID already exists. • The secure, encrypted audit trail stores all modifications made to user data.

Q & A

Question (Electronic Records)	Answer
Was an established software development life cycle used?	**Yes** The MCT4_MCTB was designed and validated using a full SDLC "risk" based system to include detailed specifications and validation of all software.
Have code reviews been conducted?	**Yes** Code reviews performed throughout validation cycle.
Has System Testing been conducted?	**Yes** All system testing complete during DVR (design verification release) validation testing and user field testing.
Has Data Conversion testing been conducted?	**Yes** Export data testing completed with signature verification of exported data performed/documented during validation.
Did validation include testing that the system discerns invalid records (i.e. invalid field entries, fields left blank that should contain data, values outside of limits, ASCII characters in numeric-only fields, etc)?	**Yes** Full security validation performed to include user login entry data, field formatting, successful/failed login attempts and audit trail functionality performed/documented during validation.
Can a copy of a single record (in electronic format) be supplied to an inspector?	**Yes** Export data testing completed with signature verification of exported data.
Is there test evidence for the audit trail functionality	**Yes** Full audit trail functionality testing performed/documented during validation.
Does test evidence exist to demonstrate the operational checks (that is, sequences of events within the system)?	**Yes** Operational check testing (include user re-authentication for operational steps) performed/documented during validation.
Does test evidence exist to demonstrate the use of the authority checks (based on role-based permissions)?	**Yes** All user and group authentication checks performed/documented during validation.

Question (Digital Signatures)	Answer
Does test evidence exist for the signature manifestation (full name, date and time)?	**Yes** Full digital signature functionality testing performed/documented during validation.
Is the transfer of the signature to another record prevented?	**No** Digital signatures are applied to a single data file only. Any attempt to alter the digital signature or transfer to another file will result in a fail during signature verification.
Does test evidence exist to document signature actions are captured in the audit trail?	**Yes** Full digital signature functionality testing performed/documented during validation.
Does test evidence exist to prove the enforcement of unique username and id?	**Yes** Full security validation performed to include user login entry data, field formatting, successful/failed login attempts and audit trail functionality performed/documented during validation.
If, when resetting the account on some systems, a "default" password is assigned, is the user forced to change the password immediately upon log on?	There is no default user/password on MCT4_MCTB device. Security setup is required by an administrator.
Are system tools used that might allow a System Administrator to falsify electronic records and/or electronic signatures?	**No** Data files are automatically signed by the system with additional signature for each file that can be added by authorized users. Administrators cannot bypass or alter the automatic system signature added to each data file.
Does the system prevent the deletion or re-assignment of a User ID after it is assigned to an electronic record?	**No** Electronic records (data files, audit trails) cannot be modified. If they are modified, they will fail the signature verification process.
Does the computerized system include functionality that requires users to periodically change their passwords (password aging)?	**Yes** Password ageing functionality testing performed/documented during validation
Does test evidence exist to demonstrate detection of attempts of unauthorized access?	**Yes** 3 attempts max. User login fails written to secure audit trail. Audit trail functionality testing performed/documented during validation
Has testing been conducted to ensure that "inactive" user accounts cannot be activated by unauthorized persons?	**Yes** Security/User functionality testing performed/documented during validation