Life Is On | Eurotherm by Schneider Electric

Eurotherm Suite Operations Server / Viewer (OPSS) and 21 CFR Part 11

Regulatory Compliance considerations

As part of the ongoing commitment to complying with 21 CFR Part 11 requirements, this data sheet is intended to demonstrate how Eurotherm uses its expertise and domain knowledge to meet the various requirements outlined in the 21 CFR Part 11 regulation. Each sub-section being considered is listed in the header of the tables below, and the statements within each table are accompanied by a commentary demonstrating how the Eurotherm solution aids compliance.

Sub Part B – Electronic Records

11.10 Controls for Closed Systems	Eurotherm Response
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:	
(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records	Eurotherm has a long history of working to formal design standards including the industry-recognized approach given in GAMP. We have many years of experience assisting our customers in achieving validation of their control systems. Our quality management and test procedures are open to your inspection and approval, with the master copy of our formal test records supplied for inclusion in your validation package.
(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.	**Trended Data** – Electronic version in daily files suitable for removal / archive – Human readable version retrievable to screen / print within the system – Conversion utility to allow DDE transfer to other applications (eg Excel) **Alarm and Event History** – Covers alarms, messages, audit trail of operator actions – Electronic version in SQL database form – Human readable version retrievable to screen / print within the system – Export utility allows text version to be taken away **Reports** – Available via Dream Report software package – Electronic version in pdf file format – Human readable both on screen and printed

Sub Part B – Electronic Records (Continued)

11.10 Controls For Closed Systems (Continued)	
(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	**Current status** Trend data and alarm and event history (including audit trail details) are read-only from normal (captive) operator interface. Trend data files for archive are in compressed (tamper resistant) format. Alarm and event history, and Audit Trail are archived into tamper resistant file. Reports in text format need protection via SOP Choice of archive media available (tape, CD, etc) **Next release** Reports in tamperproof format
(d) Limiting system access to authorized individuals.	Security system allows access to be limited both by user group (e.g. operator) and by plant area.
(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.	Runtime audit trail automatically records date/time, userID, action carried out to the alarm and event history tamper resistant file. Separate audit trail entry is generated for each action so as not to obscure previous actions and where appropriate it will record previous value before user change.. Archiving of audit trail as in (c) above.
(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Can be done by sequencing within Process Automation instruments or within InTouch scripting language
(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.	UserID and password entry are required in order to gain access as defined by user's status (user group) and the plant area being operated. Uniqueness of current user ID's is enforced automatically Read only user is supported
(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	– I/O signals can generate alarms if invalid (eg hardware malfunction, out-of-range) – Operator entered data is checked for type (alpha / numeric) and range. – Format checks can be built into underlying T-series configuration – Use of software scripts can restrict mimic and data access to defined workstation
(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.	Procedural – aided by availability of training courses from Eurotherm
(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.	Procedural – assisted by the fact that standard manuals as electronic books come as part of the Eurothermsuite installation
(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 maintain an audit trail that documents time-sequenced development and modification of systems documentation.	 Procedural Procedural

11.30 Controls For Open Systems	Not Applicable
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 Sec. 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	The product is targeted at use in closed systems.

Sub Part B – Electronic Records (Continued)

11.50 Signature Manifestations	
(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; and **(3)** The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	Add printed name as well as user ID Allow pop up request for signature with associated description and, optionally, second user confirmation Store printed name, timedate, meaning when signature is executed
(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).	Identified items will be stored in alarm and event history as described in 11.10 e

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.	Store alarm/event history (containing signature details) to tamper resistant file in order that signature cannot be excised or copied by ordinary means .

Sub Part C – Electronic Signatures

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.	No two user accounts can have the same username. Deleted user ID's cannot be re-created
(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.	Procedural
(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.	Procedural

EurothermSuite Operations Server/Viewer and 21 CFR Part 11

OpsF, OpsS and OpsW Models (applies to version 2.3)

Sub Part C – Electronic Signatures (Continued)

11.200 Electronic Signature Components And Control	
(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. **(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 period of controlled system access, each signing shall be executed using all of the electronic signature components.	Requires re-entry of user ID and password during a signing. Both components will be required for all signings
(2) Be used only by their genuine owners; and	Users can change their own passwords and no read access to passwords provided; timed logout after a period of inactivity; limit number of login retries before account is disabled; minimum length for password length; password expiry after defined number of days
(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.	Users can change their own passwords and passwords will only appear in hidden format. Administrator functions which add users or modify the account detail of other users require authorization by a second user
(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	Not applicable.

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:	
(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.	All user names are forced to be unique.
(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password ageing).	Force password expiry after defined time period. If a user leaves, account can be deleted but user ID will remain within uniqueness checks
(c) 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.	Procedural – Compromised accounts can be disabled. On loss of password, the administrator may set a new password for an account which the account holder should then immediately replace by a password of their own.
(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.	It is possible to have logins time out after a set period of inactivity; to limit the number of login retries before an account is disabled; to set a minimum length for paswords; and to force password expiry after a set number of days. Unsuccessful logins that disable accounts are detailed in the Audit Trail within the system.
(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.	Procedural

Eurotherm Limited
Faraday Close, Durrington,
Worthing, West Sussex BN13 3PL
Phone: + 44 (0)1903 268500
www.eurotherm.co.uk

Life Is On | Eurotherm by Schneider Electric