Life Is On | Eurotherm by Schneider Electric

# nanodac™

## Recorder/Controller and 21 CFR Part 11


Record Manage Optimize

### Sub Part B - Electronic Records

| 11.10 Controls for Closed Systems | |
|---|---|
| (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. | Eurotherm offer assistance with product validation to GAMP guidelines.<br><br>Files are recorded in a binary, compressed and check-summed format proprietary to Eurotherm. Details are not published. The viewing tool rejects invalid/altered (i.e. incorrectly check-summed) records.<br><br>Extensive testing is carried out by Eurotherm Ltd, an ISO 9001 approved company.<br><br>Automatic incrementing of configuration version number each time a save is changed this number is stored to the audit trail. It is also available as a maths function allowing it to be trended. |
| (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. | Complete and accurate copies are available on screen or for printing through the use of the Review software package.<br>Complete and accurate electronic copies are available by copying the raw data files or by setting up a 'PDF Printer' (requires Adobe Acrobat or similar) in order to export graphs in PDF format. |
| (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period. | On the instrument, files are held internally in Flash then archived to Removable media and/or via a network to an FTP server.<br>Data can also be periodically pulled from the product using Review.<br>Once data has left the instrument, the media it is stored on and backup strategy is the responsibility of the user. |
| (d) Limiting system access to authorized individuals. | Individual password protected user accounts. |

# nanodac™

## Recorder/Controller and 21 CFR Part 11


### Sub Part B - Electronic Records (continued)

| 11.10 Controls for Closed Systems | |
|---|---|
| (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. | Secure (embedded in the binary history file), computer generated, time-stamped runtime audit trail of batch stop/start, alarm acknowledgements, logins, signature details, configuration changes. Record changes do not obscure previous data.<br>Audit trail is embedded in the history file so guaranteeing retention alongside the records and availability for review/copying.<br>Time synchronisation is available via SNTP. |
| (f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate. | Interlocks can be achieved using the product configuration and relay outputs. The specifics are down to configuration. |
| (g) Use of authority checks to ensure that only authorised 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. | Individual password protected user accounts. Each user can have a unique set of access permissions or privileges to customise what they can do to the product. |
| (h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction. | System errors and input channel status are logged. |
| (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 - responsibility of the user |
| (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 - responsibility of the user |
| (k) Use of appropriate controls over systems documentation including:<br>(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.<br>(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation. | Procedural - responsibility of the user |

| 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. | The product is targeted at use in closed systems. With appropriate external systems/procedures the product may be used in an open system. |

# nanodac™

## Recorder/Controller and 21 CFR Part 11


| 11.50 Signature Manifestations | |
|---|---|
| (a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:<br>(1) The printed name of the signer;<br>(2) The date and time when the signature was executed; and<br>(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature. | Signed records contain username, date, time and meaning. “Meaning” includes signed/authorised information, an automatically generated type (for example, ‘config’ for a configuration change), plus an operator entered note. |
| 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). | Username, time-stamp and meaning are all embedded in the binary format history file. |

| 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. | Signature manifestation is embedded in the binary format history file. For hybrid systems, prints created via review for handwritten signature will always contain time-stamp details which permit recreation from the original data. |

## 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.<br><br>(b) Before an organisation establishes, assigns, certifies, or otherwise sanctions an individual’s electronic signature, or any element of such electronic signature, the organisation shall verify the identity of the individual | The product complies with this requirement by ensuring that no two user accounts have the same user name. Expired accounts may remain in the system and be disabled.<br><br>Procedural - responsibility of the user |
| (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.<br><br>(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.<br><br>(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 - responsibility of the user |

# nanodac™

## Recorder/Controller and 21 CFR Part 11

### Sub Part C - Electronic Signatures (continued)

| 11.200 Electronic Signature Components and Controls | |
|---|---|
| (1) Employ at least two distinct identification components such as an identification code and password.<br>(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.<br>(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 name 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 is provided. It is also 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 passwords; and to force password expiry after a set 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 no read access to passwords is provided. So, unless one user tells another their password, it is impossible to commit fraud without an audit trail of that fraud being left. It is further possible to force system administrator changes for user accounts to be authorized by a second individual. |

| 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. | Providing user accounts are not deleted then 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 aging). | It is possible to force password expiry after a set number of days. If a user leaves, their account can be disabled. |
| (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 unauthorised 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 passwords; and to force password expiry after a set number of days. Failed logins that disable accounts are detailed in the Audit Trail within the instrument. |

**Eurotherm Limited**
Faraday Close, Durrington,
Worthing, West Sussex BN13 3PL
Phone: + 44 (01903) 268500
Fax: + 44 (01903) 265982
**www.eurotherm.com**

Life Is On Eurotherm by Schneider Electric

Document Number HA032921 Issue 1 © 2016 Schneider Electric. All rights reserved. All trademarks are owned by Schneider Electric Industries SAS or its affiliated companies.