White paper

# CA79 TOC analyzer / 21CFR Part 11 Statement

21 Code of Federal Regulations Part 11,
21 CFR Part 11 Statement

**Author**
Endress+Hauser Liquid Analysis
Endress+Hauser Life Sciences Project Support

Endress+Hauser

| | |
|---|---|
| **Equipment** | **TOC Analyzer CA79, device model A2** |
| **Manufacturer** | **Endress+Hauser Conducta GmbH+Co. KG, Germany** |
| **Operating system** | **MS-Windows® compatible (Windows 10 Pro)** |
| **Manufacturer** | **Endress+Hauser Conducta GmbH+Co. KG,<br>Dieselstrasse 24, 70839 Gerlingen, Germany** |

| **Part 11 Section** | System requirements | Comments |
|---|---|---|
| **1. Subpart A - General Provisions** | | |
| **§ 11.1** | Scope | |
| **§ 11.2** | Implementation | |
| **§ 11.3** | Definitions | |
| **2. Subpart B - Electronic Records** | | |
| **§ 11.10** | Controls for closed systems | |
| 11.10(a) | Is the system validated to ensure accuracy, reliability, and consistent intended performance? | Yes. |
| 11.10(a) | Is the system validated to ensure the ability to discern invalid or altered records?<br>▪ Does the system ‘flag’ invalid records?<br>▪ Does the audit trail track altered records? | Yes.<br>Invalid records are not saved / existent and therefore a ‘flag’ is not required.<br>As all data are immediately and permanently stored in an encrypted format, there is no such thing as altered records. No user, also not the admin has access to the measuring data. |
| 11.10(b) | Is the system capable of producing accurate and complete copies of records in human readable and electronic format for inspection, review and copying by the regulatory agency?<br>▪ Can records be extracted in a format that can be read by the regulatory agency?<br>▪ Are annotations (e.g. “comments”) included as part of the record? | Yes.<br>Records can be displayed and printed. The device software provides capabilities of converting the proprietary, encrypted format of electronic records into the common human readable „.CSV“ or „PDF“ format.<br>The (converted) electronic records contain complete data, including the audit trail. The exported data are not the raw data anymore. The data which are in the database are the raw data.<br>Annotations / “comments” can be added as a part of the record. |
| 11.10(c) | Are the records protected to enable their accurate and ready retrieval throughout their retention period? | Yes.<br>All measuring and calibration data and all user interactions are permanently stored on the device. The data are encrypted immediately. They can be returned into a human readable format by a read-only-software called “Viewer”. Data review is considered “tamper-proof”. A later modification of the audit trail data is not possible. |

| | | |
|---|---|---|
| 11.10(d) | Is system access limited to authorized individuals?<br>▪ How are users authorized to get access?<br>▪ How is access modification and deletion managed?<br>▪ Is access periodically checked?<br>▪ Does the system provide adequate security?<br>▪ Do different access levels exist? | Yes.<br>The device differentiates between users.<br>Using unique password-/ID combinations access to different functionality is controlled.<br>The password-/ID combinations need to be periodically renewed (forced by the device).<br>The Administrator (System Owner) is responsible for the systems availability and can add new users using one unique ID or deactivate old users. It is not possible to delete user profiles.<br>The information of deactivated user profiles will still be stored on the device. This prevents the "re-use" of deactivated user ID/password combinations.<br>There are 3 clearly defined user levels, "Admin", "Operator" and "Assistant".<br>To change any parameter, the user needs to leave the automatic "measuring mode". This will be documented in the audit trail. When the measuring mode is stopped, no new TOC values are generated, and no TOC value is shown on the display. To restart the measuring mode, the user needs to identify again by the unique user ID / password combination.<br>Any user interaction requires a user identification which is password-protected. Changes of the device configuration will be documented in the audit trail.<br>"Operator" and "Assistant" user levels have access only to specified operations. Neither the Administrator nor the Operator has access to manipulate the measured values or audit trail. |
| 11.10(e) | Is there a secure, computer generated, time stamped audit trail that independently records the date and time of operator entries and actions that create, modify, or delete electronic records?<br>▪ Is the audit trail protected from intentional or accidental modification?<br>▪ Is the audit trail always on?<br>▪ Is the audit trail computer generated?<br>▪ Is the date and time recorded? Is the time local to the activity? Is it protected from unauthorized change? Is time recorded to the second?<br>▪ Is the operator name captured?<br>▪ Does the audit trail track operator entries and action that create, modify or delete records? Can the type of action be determined from the audit trail? | Yes.<br>The computer-generated audit trail function is always activated. It is protected from intentional or accidental modification.<br>The System Time is documented to each activity and recorded to the second. The system time shall be compared and synchronized to the PLC time server manually on a regular basis.<br>The audit trail does track operator entries including operator name (ID) and actions that create new entries. A modification of stored records is not possible.<br>The type of action can be determined from the audit trail.<br>A modification of stored data in the software is not possible. User actions include a comment. The comment is marked as user comment.<br>The Audit Trail cannot be deactivated. |
| 11.10(e) | Upon making a change to an electronic record, is previously recorded information still available (i.e. not obscured by the change)? | Yes.<br>Changes always create a new record. Previously recorded information is still available. |

| | | |
|---|---|---|
| 11.10(e) | Is an electronic record's audit trail retrievable throughout the record's retention period? | Yes.<br>The entire audit trail is retrievable throughout the record's retention period. A user cannot delete audit trail information. The retention period is longer than the expected lifetime of the device (> 15 years). |
| 11.10(e) | Is the audit trail available for review and copying by the FDA?<br>▪ Can the audit trail be printed?<br>▪ Can records be extracted in an electronic format that can be read by FDA? | Yes.<br>The audit trail can be printed and exported as a .pdf file.<br>Audit trail records are stored in an encrypted, electronic format that can be displayed by the "Viewer" software. The "Viewer" software is a "read only" software and cannot be used for modifications. |
| 11.10(f) | If the sequence of system steps or events is important, is this enforced by the system (e.g. data must be entered before it can be approved)? | Yes.<br>The system software does not allow entering commands/comments before the user has successfully logged in.<br>Operational system checks: Guidance for the operator via a menu driven user menu.<br>Only authorized users are allowed to view and export records. |
| 11.10(g) | Are there checks in place 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?<br>▪ How are users authorized to get access?<br>▪ How is access modification and deletion managed?<br>▪ Is access periodically checked?<br>▪ Does the system ensure adequate security?<br>▪ Do different access levels exist? Are they documented? Are they enforced by the system? | Yes.<br>The User management differentiates 'Administrator' and two lower authorization levels for access purposes.<br>System access and modification are allowed only by the individual user ID and password combination. The "Admin" can add or deactivate users of a lower hierarchy level, by using the individual ID / password combination. All three user levels have individual rights. Each user ID is assigned to one of the three user levels. The access levels are automatically enforced with every login. All measuring data are stored permanently. There is no possibility to modify a record. All passwords have a defined validity and do expire. |
| 11.10(h) | If it is a requirement of the system that input data or instructions can only come from certain input devices, does the system check the validity of the source of data input or operational instructions? | Yes.<br>The CA79 does not process any data from external sources like sensors. There is no way to import measuring data from external sources into the system. |
| 11.10(i) | Has it been determined and properly documented that persons who develop, maintain, or use electronic record/ electronic signature systems have the education, training, and experience to perform their assigned tasks? | Yes.<br>The team is trained in 21 CFR Part 11 requirements and GMP regulations and guidelines. |
| 11.10(j) | Are there written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification? | N/A<br>(This is the responsibility of the user/company.) |
| 11.10(k)(1) | Do adequate controls exist over the documentation for the distribution of, access to, and use of systems operation and maintenance documentation controlled? | N/A<br>(This is the responsibility of the user/company.) |

| | | |
|---|---|---|
| 11.10(k)(2) | Do revision and control procedures exist to maintain an audit trail that documents time-sequenced development and modification of systems documentation? | Yes.<br>The audit trail of the analyzer is stored instantaneously in an encrypted format, that cannot be modified later. The "Viewer" software has "read only" functionality.<br>N/A.<br>(Revision procedures for derived reports are in the responsibility of the user/company.) |
| **§ 11.30** | Controls for open systems | |
| 11.30 | Do procedures and controls exist, as necessary in an open system, to ensure record authenticity, integrity, and confidentiality from the point of record creation to the point of receipt?<br>■ Is document encryption used?<br>■ Are digital signature standards used?<br>■ Are other controls required? | N/A<br>The TOC software is a closed system. The access to it is controlled by the 3-level user management and individual passwords. All audit trail data are encrypted immediately. The recorded data can be printed as a pdf file or they can be displayed by the "Viewer" software which has a "read only" functionality. Modifications of the recorded data are not possible.<br>No other controls are required. |
| **§ 11.50** | Signature manifestations | |
| 11.50(a) | Do signed electronic records contain information associated with the signing that clearly indicates:<br>1. The printed name of the signer?<br>2. The date and time when the signature was executed?<br>3. The meaning of the signing associated with the signature?<br>■ Are date and time applied by the data manager?<br>■ Is the time local to the signing?<br>■ Is the time protected from unauthorized change?<br>■ Is time recorded to the second? | Yes.<br>Recorded data are automatically assigned to the responsible user identified by his electronic signature and can be reviewed.<br>The signature contains the unique user ID and the date and time of the user login, automatically generated by the system. The time is recorded to the second.<br>N/A.<br>The administration of individual user IDs and passwords linked to names is the responsibility of the customer / company. |
| 11.50(b) | Are items 1, 2, and 3 above subject to the same controls as for electronic records and included as part of any human readable form of the electronic record? | Yes.<br>Recorded user actions are automatically assigned to the responsible user identified by his unique user ID. The audit trail can be reviewed in human readable format either direct at the unit or by the "Viewer" software. |
| **§ 11.70** | Signature/record linking | |
| 11.70 | Are electronic signatures and handwritten signatures executed to electronic records linked to their respective electronic records to ensure that the signature cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means?<br>■ How is the record and signature linked?<br>■ Is the signature protected to prevent transfer to another record?<br>■ Is the signed record protected to prevent changes after signing?<br>■ If the record is changed, is the signer prompted to re-sign following the change? | Yes.<br>As there is only one ongoing audit trail on the CA79 device, that is stored during the whole lifetime of the device, some of the questions are not relevant. The complete audit trail, including all user actions, are immediately stored and cannot be modified later. Reports can be generated and exported at any time. These reports can be printed out and signed by individual users. However, other users and auditors can generate the same report any time later, again. As there is only one permanent version of the audit trail, the data reliability is guaranteed. The "Viewer" software for the creation of the reports is a "read only" software and will therefore not change the audit trail. |

| **Part 11 Section** | System requirements | Comments |
|---|---|---|
| **2.1 Subpart C - Electronic Signatures** | | |
| **§ 11.100** | General requirements | |
| 11.100(a) | ■ Is each electronic signature unique to one individual?<br>■ Is an electronic signature ever re-used by, or reassigned to, anyone else? | Yes.<br>Each user account is unique to one individual. The CA79 TOC analyzer software maintains a list of active and deactivated user accounts. Therefore, it is not possible to re-use or reassign individual user IDs. |
| 11.100(b) | Is the identity of an individual verified before establishing, assigning, certifying, or otherwise sanctioning an individual's electronic signature, or any element of such electronic signature? | N/A<br>(This is the responsibility of the user/company.) |
| 11.100(c) | Has the user notified the regulatory agency that the electronic signatures in its system are intended to be the legally binding equivalent of traditional handwritten signatures? | N/A<br>(This is the responsibility of the user/company.) |
| 11.100(c) | If electronic signatures are being used, can additional certification or testimony be provided that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature?<br>■ Is there any documentation to support that individuals understand that electronic signatures are the legally binding equivalent of their handwritten signatures? | N/A<br>(This is the responsibility of the user/company.) |
| **§ 11.200** | Electronic signature components and controls | |
| 11.200(a)(1) | Is the non-biometric signature made up of at least two (2) distinct identification components, such as an identification code and password? | Yes.<br>The electronic signature consists of one unique identification code (ID) and one password. |
| 11.200(a)(1)(i) | When an individual executes a series of signings during a single, continuous period of controlled system access, is the first signing executed using all electronic signature components, and subsequent signings are executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual?<br>■ Are both electronic signature components required for the first signing?<br>■ Is the period of continuous use defined?<br>■ Does the system log off after a period of inactivity?<br>■ If only one component is required (as in subsequent signings), is it the private component? | Yes.<br>The combination of both components, User ID and password are requested in any case. Every user interaction (parameter settings, comments, rights management, start of measurement, qualification etc.) require a new identification. Both components ID and password are required newly for each activity. Therefore, each individual action can be allocated to one individual user.<br>During standard operation, the CA79 is in the automatic measuring mode. In this mode, no settings or parameters can be modified. For user interactions, the user needs to end the measuring mode, first. For this purpose, he needs to identify with user ID and password. Only after, users can modify settings, but need to identify for every single screen. With leaving a particular screen, the user is logged off immediately. The restart of the measuring mode required again the unique user ID / password combination for identification. |

| | | |
|---|---|---|
| 11.200(a)(1)(ii) | When an individual executes one or more signings not performed during a single, continuous period of controlled system access, is each signing executed using all the electronic signature components? | Yes.<br>The access to CA79 always requires both components user ID and password. |
| 11.200(a)(2) | Are non-biometric signatures used only by their genuine owners?<br>▪ Are there procedures and training to reinforce that non-biometric electronic signatures are to be used only by their genuine owners (not shared, not loaned, not borrowed, not posted)? | N/A<br>(This is the responsibility of the user/company.) |
| 11.200(a)(3) | Are non-biometric signatures 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?<br>▪ Could one person be working alone "forge" another person's electronic signature? | N/A<br>(This is the responsibility of the user/company.) |
| 11.200(b) | Are electronic signatures based upon biometrics designed to ensure that they cannot be used by anyone other than their genuine owners? | N/A<br>(This is the responsibility of the user/company.) |
| **§ 11.200** | Controls for identification codes/passwords | |
| 11.300(a) | Are controls in place to maintain the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password?<br>▪ Is uniqueness ensured historically as well as currently?<br>▪ Does the process of assigning accounts ensure uniqueness?<br>▪ Does the system prevent re-use of usernames? | Yes.<br>The CA79 software ensures that all authorized electronic signatures are unique. All active and deactivated user accounts are stored permanently on the device. A re-use of user ID would not be accepted by the device. (Identification code and Password maintenance is the responsibility of the user.) |
| 11.300(b) | Is the issuance of identification codes and passwords periodically checked, recalled, or revised (e.g. to cover such events such as password aging)?<br>▪ Do passwords periodically expire and need to be revised?<br>▪ Is there a procedure for recalling identification codes and passwords if a person leaves or is transferred? | Yes.<br>CA79 can be set up to monitor password aging or expirations. The user must renew his/her password in a specified cycle (e.g. every 30 days). The 'Administrator' has the authority to add/deactivate the Identification code and Password for authorized users. The password can not be recalled for safety purposes. |
| 11.300(c) | Are there loss management procedures to electronically de-authorize 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? | N/A<br>This is the responsibility of the user/company. (The software offers possibilities for the administrator to deactivate user profiles.) |

| | | |
|---|---|---|
| 11.300(d) | Are there 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?<br>▪ Does the system prevent unauthorized access?<br>▪ Are break-in attempts monitored? | Yes.<br>The CA79 TOC software prevents unauthorized access. A defined number of password retries (adjustable) will lead to the deactivation of the user. Each login attempt will be recorded. As the CA79 is a stand-alone unit with no remote access, automated access retries are not possible. The access control to the location is a second safeguard.<br>(Additional or other transaction safeguards are the responsibility of the user.) |
| 11.300(e) | Are there procedures covering the 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? | N/A<br>Tokens or cards, which bear or generate identification code or password information, are not used. |

www.addresses.endress.com

Endress+Hauser
People for Process Automation