WHITE PAPER

21 CFR Part 11 & Annex 11 Statement for GMP Pharmaceutical Washers and Sterilizers

Using WinCC Unified Software

Objective

This document provides the statement of compliance of our GMP pharmaceutical washers and sterilizes controlled by WinCC Unified software to 21 CFR Part 11 and Annex 11 standards.

- 21 CFR Part 11 covers electronic records and electronic signatures for the FDA (FDA: Food and Drug Administration, CFR: Code of Federal Regulations, Title 21: Food and Drugs, Part 11: Electronic Records, Electronic Signature)
- Annex 11 focuses on the lifecycle of computerized systems for human and veterinary medicinal products manufactured in the European Union

The following sections describe Subpart B of Part 11 for electronic records and Subpart C of Part 11 for electronic signatures.

Definitions and terminology

Regulation terminology

- Biometrics: a method of verifying an individual's identity based on measurement of their physical feature(s) or repeatable action(s) unique to that individual and measurable.
- Closed system: an environment in which system access is controlled by persons responsible for the content of electronic records.
- Computerized system: a system including the input of data, electronic processing, and the output of information used for reporting or automatic control.
- Electronic record: any digital form representation of text, graphics, data, audio, pictorial, or other information created, modified, maintained, archived, retrieved, or distributed by a computer system.
- Electronic signature: a computer data compilation of symbols adopted by an individual to be the legally binding equivalent of a handwritten signature.

Getinge terminology

- URS: User Requirement Specification
- FS: Functional Specification
- SDS: Software Design Specification
- AD: Active Directory
- QMS : Quality Management System

Description

Our GMP pharmaceutical washers and sterilizers utilize the WinCC Unified software proposed by Siemens.
The following compliance statements are derived from the ERES Compliance Response for SIMATIC WinCC Unified V20.

Version History

Date	Revision	Written/Updated by	Description
12 JUN 2025	001	Amaury BRICOUT	Original release

Internal approval

Name	Department	Date	Signature
Marcus Persson	Automation Sterilizers		
Manuel Samsom	Automation Washers		

Customer approval

Name	Role	Date	Signature

Table 1: Subpart B – Electronic Records

21 CFR Part 11 Requirements	Annex 11	Compliant	Application notes
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. Such procedures and controls shall include the following:	**7.1** – Data should be secured by both physical and electronic means against damage. **7.2** – Regular back-ups of all relevant data should be done. **12.1** – Physical and/or logical controls should be in place to restrict access to computerized systems to authorized persons.	☒ Yes ☐ No ☐ N/A	The Getinge documentation is generated, maintained, recorded and delivered to the customer to describe system design (Functional Specification, Hardware Design Specification, Software Design Specification) and validation (FAT/SAT protocol). All records are stored in a database and are available for viewing, printing, and exporting throughout the records retention period. A backup procedure is provided in the service manual to the customer. Automatic backup of data base can be configured (optional). User access rights to the report is provided by a user group right. Group roles are specified in the design documentation. Local user accesses are managed by UMC. Access to the active directory with UMC is optional. Physical controls to restrict access to the system is in the scope of the final customer.
11.10(a) – Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	**4.1** – Validation documentation and reports should cover the relevant steps of the life cycle. Manufacturers should be able to justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment.	☐ Yes ☐ No ☒ N/A	The validation of Getinge software applications is made according to Getinge QMS. A traceability matrix is delivered (optional). Although the system is ready for compliance with 21 CFR Part 11, the end user is responsible for the validation of the overall system. Getinge can offer support for the validation of the system.
N/A	**4.2** – Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process.	☒ Yes ☐ No ☐ N/A	Deviations observed during the validation process are tracked. Non-conform test executions are recorded and linked to the test plan. If a change is necessary, a Getinge change procedure is applied.

21 CFR Part 11 Requirements	Annex 11	Compliant	Application notes
N/A	**4.3** – An up-to-date listing of all relevant systems and their GMP functionality (inventory) should be available. For critical systems, an up- to-date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures	☒ Yes ☐ No ☐ N/A	The Getinge documentation is generated, maintained, recorded and delivered to the customer to describe system design (Functional Specification, Hardware Design Specification, Software Design Specification)
N/A	**4.5** – The regulated user should take all reasonable steps to ensure that the system has been developed in accordance with an appropriate quality management system.	☒ Yes ☐ No ☐ N/A	A procedure is applied to adapt the template project to the washer or sterilizer project. A software adaptation form or equivalent is done by an automation engineer. A source code review is done by another automation engineer.
N/A	**4.7** – Evidence of appropriate test methods and test scenarios should be demonstrated. Particularly, system (process) parameter limits, data limits and error handling should be considered. Automated testing tools and test environments should have documented assessments for their adequacy.	☒ Yes ☐ No ☐ N/A	Tests to validate the washer and sterilizer software are performed according to QMS.
N/A	**4.4** – User Requirements Specifications should describe the required functions of the system, be based on documented risk assessment and GMP impact, and be traceable throughout the life cycle.	☐ Yes ☐ No ☒ N/A	URS is delivered by customer. A traceability matrix is delivered (optional).
N/A	**4.6** - For the validation of bespoke or customized computerized systems there should be a process in place that ensures the formal assessment and reporting of quality and performance measures for all the life-cycle stages of the system.	☐ Yes ☐ No ☒ N/A	Tests to validate the washer and sterilizer softwares are performed according to QMS. Although the system is ready for compliance with Annex 11, the end user is responsible for the validation of the overall system. Getinge can offer support for the validation of the system.

21 CFR Part 11 Requirements	Annex 11	Compliant	Application notes
N/A	**4.8** – If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process.	☐ Yes ☐ No ☒ N/A	The reading of raw data in the Getinge system is in the scope of customer (Data exchange table and SQL Data Base). OPC UA and Profinet communication protocols are available (option).
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. 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.	**8.1** – It should be possible to obtain clear printed copies of electronically stored data.	☒ Yes ☐ No ☐ N/A	All records are stored in a database. The system allows to generate batch, recipe, audit trail and alarm log reports in PDF format.
11.10(c) – Protection of records to enable their accurate and ready retrieval throughout the records retention period.	**7.1** – Data should be secured by both physical and electronic means against damage. Access to data should be ensured throughout the retention period. **7.2** – Regular back-ups of all relevant data should be done. **8.1** – It should be possible to obtain clear printed copies of electronically stored data. **12.1** – Physical and/or logical controls should be in place to restrict access to computerized systems to authorized persons.	☒ Yes ☐ No ☐ N/A	All records are stored in a database and are available for viewing, printing, and exporting throughout the records retention period. A backup procedure is provided in the service manual notice to the customer. Automatic backup of data base can be configured (optional) User access rights to the report is provided by a user group right. Group roles are specified in the design documentation. Local user accesses are managed by UMC. Access to active directory with UMC is optional.

21 CFR Part 11 Requirements	Annex 11	Compliant	Application notes
11.10(d) – Limiting system access to authorized individuals.	**2** – All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties. **12.1** – Physical and/or logical controls should be in place to restrict access to computerized systems to authorized persons. Suitable methods of preventing unauthorized entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas. **12.3** – Creation, change, and cancellation of access authorizations should be recorded.	☒ Yes ☐ No ☐ N/A	Only authorized individuals with a valid user name and password can log to the system. A password policy (complexity, expiration delay) is specified in the FS and configured in the system. Only administrators have possibility to exit the application. Local user accesses are managed by UMC. Access to active directory with UMC is optional. Creation, change, and cancellation of access authorizations for Active Directory are in the customer scope.
11.10(e) – Use of secure, computer-generated, timestamped 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.	**7.1** – Access to data should be ensured throughout the retention period. **9** – Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail"). For change or deletion of GMP-relevant data the reason should be documented. Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed. **12.4** – Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleted data including date and time.	☒ Yes ☐ No ☐ N/A	SIMATIC WinCC Unified supports the requirement for an audit trail of GMP-relevant operator actions by recording these actions accordingly (who, what, when, and optionally why). Such electronic recordings are secured through system-side security mechanisms. Timestamps are stored in UTC format. See Audit Trail Appendix 1 for further details.
11.10(f) – Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	**N/A** (no direct Annex 11 counterpart).	☒ Yes ☐ No ☐ N/A	Software are validated prior to being handed over to the customer.

21 CFR Part 11 Requirements	Annex 11	Compliant	Application notes
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.	**2** – All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties. **12.1** – Physical and/or logical controls should be in place to restrict access to computerized systems to authorized persons. Suitable methods of preventing unauthorized entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas.	☒ Yes ☐ No ☐ N/A	Only authorized individuals with a valid user name and password can log in to the system. A password policy (complexity, expiration delay) is specified in the FS and configured in the system. Only administrators have possibility to exit the application. Local user accesses are managed by UMC. Access to active directory with UMC is optional.
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.	**6** – For critical data entered manually, there should be an additional check on the accuracy of the data. This check may be done by a second operator or by validated electronic means.	☒ Yes ☐ No ☐ N/A	The equipment undergoes testing and FAT under production environment prior to being installed at customer site. During this validation, Inputs/Outputs are verified.
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.	**2** – All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties.	☐ Yes ☐ No ☒ N/A	Getinge checks that persons respect the Getinge SOP and coding rules. The end user is responsible for hiring and training appropriate staff members with the education, training, and experience to perform assigned tasks. Getinge can offer training and support throughout the life cycle of the system.
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.	**N/A** (no direct Annex 11 counterpart).	☐ Yes ☐ No ☒ N/A	The requirement for policies that hold individuals accountable and responsible for actions initiated under their electronic signatures is a customer procedural requirement.

21 CFR Part 11 Requirements	Annex 11	Compliant	Application notes
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 maintain an audit trail that documents time-sequenced development and modification of systems documentation.	**N/A** (no direct Annex 11 counterpart to 21 CFR 11.10(k)(1)). **10** – Any changes to a computerized system including system configuration should only be made in a controlled manner in accordance with a defined procedure.	☐ Yes ☐ No ☒ N/A	Getinge provides project documentation and software for customer review. Modification of software is described in a procedure and a document is created to record old and version of software/documentation. This form and new software/documentation are provided to the customer. End users are responsible for providing procedural controls for access, distribution and use of the documents for the lifetime of the system. End users should define adequate change control procedures for operational and maintenance of documentation.
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.	**5** – Computerized systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks. **7.1** – Data should be secured by both physical and electronic means against damage. **7.2** – Regular back-ups of all relevant data should be done. **12.1** – Physical and/or logical controls should be in place to restrict access to computerized systems to authorized persons.	☐ Yes ☐ No ☒ N/A	Washers and sterilizers have limited connection to other systems: Connection to Customer active Directory (optional): Customer scope management Data exchange table (optional): Getinge use industrial protocols (Ethernet/IP, OPC UA) to secure communication. A backup procedure is provided in the service manual to the customer. Automatic backup of data base can be configured (optional) Only authorized individuals with a valid user name and password can log to the system. A password policy (complexity, expiration delay) is specified in the FS. Local user accesses are managed by UMC. Access to active directory with UMC is optional. End users are responsible for establishing internal policies and procedures to ensure appropriate controls if system are to beclassified as an open system.

21 CFR Part 11 Requirements	Annex 11	Compliant	Application notes
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; and (4) 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).	**14** – Electronic records may be signed electronically. Electronic signatures are expected to have the same impact as hand-written signatures, be permanently linked to their respective record, and include the time and date that they were applied.	☒ Yes ☐ No ☐ N/A	The listed information is available. See Electronic Signature appendix 2 for more details.
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.	**14** – Electronic signatures are expected to be permanently linked to their respective record.	☒ Yes ☐ No ☐ N/A	The electronic signatures cannot be removed or used in any other way. See Electronic Signature appendix 2 for more details. The end user should establish SOPs to enforce this requirement upon archived records.

Table 2: Subpart C – Electronic Signatures

21 CFR Part 11 Requirements	Annex 11	Compliant	Application notes
11.100(a) – Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	**N/A** (no direct Annex 11 counterpart).	☒ Yes ☐ No ☐ N/A	The electronic signature uses the unique identifiers for user accounts. The re-use or re-assignment of electronic signatures is effectively prevented.
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.	**N/A** (no direct Annex 11 counterpart).	☐ Yes ☐ No ☒ N/A	The customer should establish appropriate procedural controls for the verification of an individual's identity before allocating a user account and/or electronic signatures.
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, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.	**14.a** –Electronic signatures are expected to have the same impact as hand-written signatures.	☐ Yes ☐ No ☒ N/A	Customers are responsible for notifying the FDA of their intention of recognizing the electronic signature to be a legally binding equivalent of traditional handwritten signatures.

21 CFR Part 11 Requirements	Annex 11	Compliant	Application notes
11.200(a)(1) – Electronic signatures that are not based upon biometrics shall: **(i) employ at least two distinct identification components such as an identification code and password,** **(ii) 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.** **(iii) 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.**	**12.1** – Physical and/or logical controls should be in place to restrict access to computerized. systems to authorized persons. Suitable methods of preventing unauthorized entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas.	☒ Yes ☐ No ☐ N/A	Performing an electronic signature requires the user ID as well as the user's password. See Electronic Signature appendix 2 for more details.
11.200(a)(2) – Electronic signatures that are not based upon biometrics shall be used only by their genuine owners.	**12.1** – Physical and/or logical controls should be in place to restrict access to computerized. systems to authorized persons. Suitable methods of preventing unauthorized entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas.	☐ Yes ☐ No ☒ N/A	The customer is responsible for ensuring that the genuine owner is signing the electronic signature and that the password is not being disclosed to others.

21 CFR Part 11 Requirements	Annex 11	Compliant	Application notes
11.200(a)(3) – Electronic signatures that are not based upon biometrics shall 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.	**12.1** – Physical and/or logical controls should be in place to restrict access to computerized systems to authorized persons. Suitable methods of preventing unauthorized entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas.	☐ Yes ☐ No ☒ N/A	The customer should implement appropriate procedures to handle situations that require an electronic signature by anyone other than its genuine owner. The electronic signature uses the unique identifiers for user accounts. The re-use or re-assignment of electronic signatures is effectively prevented Performing an electronic signature requires the user ID as well as the user's password Each signature consists of two components (user ID and password). It is not possible to falsify an electronic signature during signing or after recording of the signature. In addition, the regulated user needs procedures that prevent the disclosure of passwords.
11.200(b) – Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	**12.1** – Physical and/or logical controls should be in place to restrict access to computerized systems to authorized persons. Suitable methods of preventing unauthorized entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas.	☐ Yes ☐ No ☒ N/A	Biometric-based logon mechanisms are not available on the system.
11.300(a) – 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.	**12.1** – Physical and/or logical controls should be in place to restrict access to computerized systems to authorized persons. Suitable methods of preventing unauthorized entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas.	☒ Yes ☐ No ☐ N/A	Security of user management is ensured by WinCC Unified Administration tools. User management can be linked to the customer Active Directory (optional) Uniqueness of users and roles are in the scope of customer.

21 CFR Part 11 Requirements	Annex 11	Compliant	Application notes
11.300(b) – Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	**11** – Computerized systems should be periodically evaluated to confirm that they remain in a validated state and are compliant with GMP. Such evaluations should include, where appropriate security. **12.3** – Creation, change, and cancellation of access authorizations should be recorded.	☒ Yes ☐ No ☐ N/A	A password policy (complexity, expiration delay) is specified in the FS and configured in the system. Management of users and roles are in the scope of customer.
11.300(c) – Following 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.	**12.3** – Creation, change, and cancellation of access authorizations should be recorded.	☐ Yes ☐ No ☒ N/A	Customer procedures must be established to meet this requirement. Getinge does not use tokens, cards, or other devices that bear or generate identification code or password information.
11.300(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.	**12.1** – Physical and/or logical controls should be in place to restrict access to computerized systems to authorized persons.	☒ Yes ☐ No ☐ N/A	Any log entry (failed or complete) is recorded in the audit trail. A password policy (complexity, expiration delay) is specified in the FS and configured in the system. An account lockout threshold is configured.
11.300(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 been altered in an unauthorized manner.	**11** – Computerized systems should be periodically evaluated to confirm that they remain in a validated state and are compliant with GMP. Such evaluations should include, where appropriate . . . security.	☐ Yes ☐ No ☒ N/A	Getinge does not use tokens, cards, or other devices that bear or generate identification code or password information.

21 CFR Part 11 Requirements	Annex 11	Compliant	Application notes
N/A (No direct 21 CFR Part 11 counterpart)	**13** - All incidents, not only system failures and data errors, should be reported and assessed. The root cause of a critical incident should be identified and should form the basis of corrective and preventive actions.	☐ Yes ☐ No ☒ N/A	Reporting of system incidents is out of Getinge scope.
N/A (No direct 21 CFR Part 11 counterpart)	**15** - When a computerized system is used for recording certification and batch release, the system should allow only Qualified Persons to certify the release of the batches and it should clearly identify and record the person releasing or certifying the batches. This should be performed using an electronic signature.	☐ Yes ☐ No ☒ N/A	Batch release functionality is out of Getinge scope
N/A (No direct 21 CFR Part 11 counterpart)	**16** - For the availability of computerized systems supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (e.g. a manual or alternative system). The time required to bring the alternative arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequately documented and tested.	☒ Yes ☐ No ☐ N/A	After completion of SAT, issues with the equipment are handled by local service team.

Appendix 1

SIMATIC WinCC Unified Audit Trail

Introduction

The Audit Trail feature in SIMATIC WinCC Unified V20 is a crucial component for ensuring compliance with Electronic Records and Electronic Signatures (ERES) regulations. It supports the requirement for a secure, reliable, and traceable system that records operator actions in GMP-relevant processes. It is not possible for the user to deactivate audit trail functionality.

Audit Trail functionality

The Audit Trail records all changes and inputs made by the operator during the system's operation. These records include essential details such as:

- Who: Identification of the operator making the changes.
- What: Description of the action performed.
- When: Time stamp indicating when the action occurred.
- Why: Optional reason for the change.

System security

Changes to the system configuration are managed separately and subject to a change control procedure. This process includes planning, impact evaluation, documentation, and testing for correct implementation. The system ensures that all recorded information remains secure and cannot be altered or deleted by the operator.

Operational recordings

The system distinguishes between automatically generated records, which do not require an audit trail, and operator-generated records, which are subject to audit trail requirements. The SIMATIC WinCC Unified Audit option package allows the configuration of GMP-relevant variables to be tracked in the audit trail.

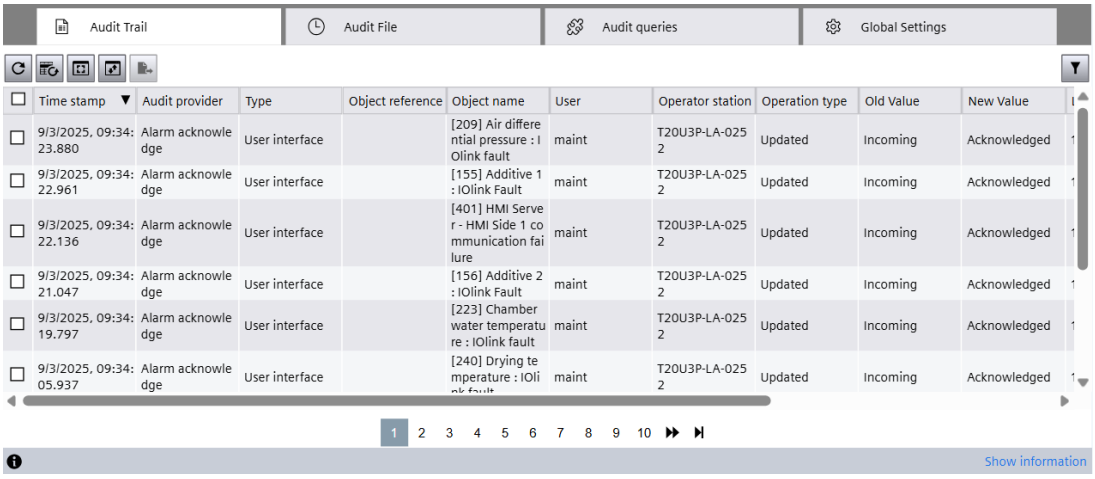

Figure 1: Some of the available fields in the audit trail

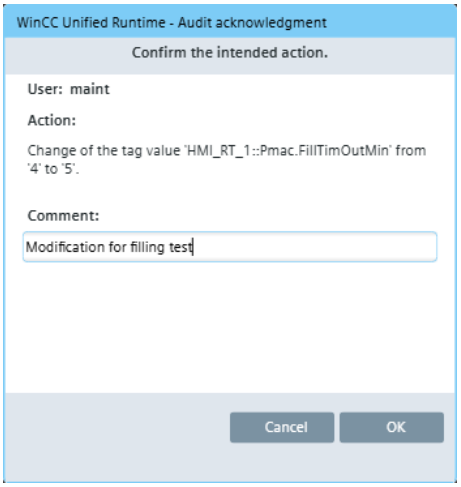

Figure 2: Entering a comment when performing a change on a GMP setting

Audit Viewer

The Audit Viewer in WinCC Unified displays audit trail data in Runtime, allowing operators and regulators to review the recorded actions.

Every audit trail entry is secured with an integrated checksum. The Audit Viewer can detect any manipulation made and also state which audit trail entry that has been manipulated.

Parameter control

SIMATIC WinCC Unified also supports the storage of actions via parameter control (PaCo). Operator actions such as downloading parameter sets and changing individual parameters are recorded accordingly.

Compliance and documentation

The audit trail feature meets the requirements of both 21 CFR Part 11 and Annex 11 of the EU-GMP Guidelines. It ensures that electronic records and electronic signatures are as reliable and trustworthy as their paper counterparts, providing a secure and traceable system for regulatory compliance.

Conclusion

The Audit Trail in WinCC Unified is a comprehensive solution for maintaining data integrity and traceability in GMP-relevant processes. By recording operator actions and changes to the system configuration, it provides a secure and compliant environment for electronic records and signatures.

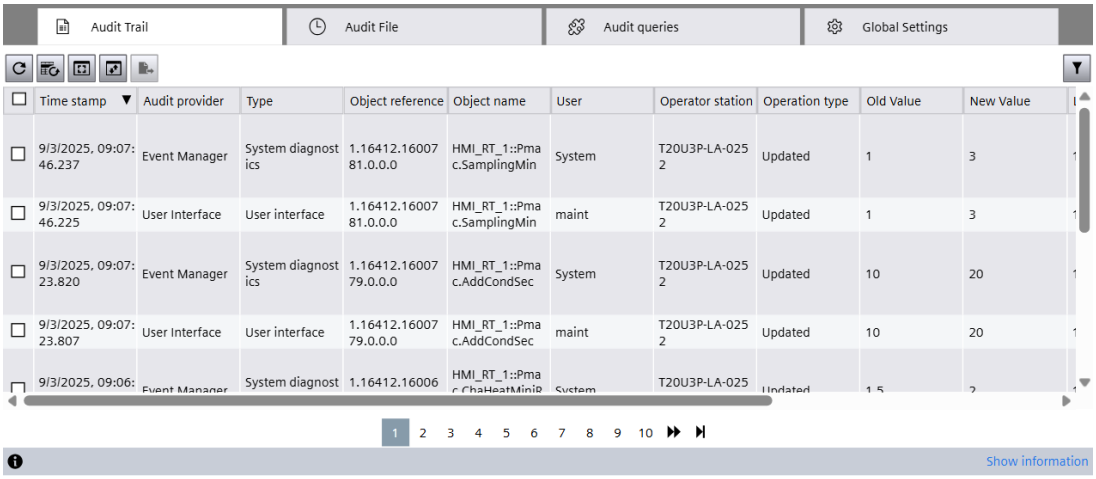

Figure 3: Audit viewer in WinCC Unified system

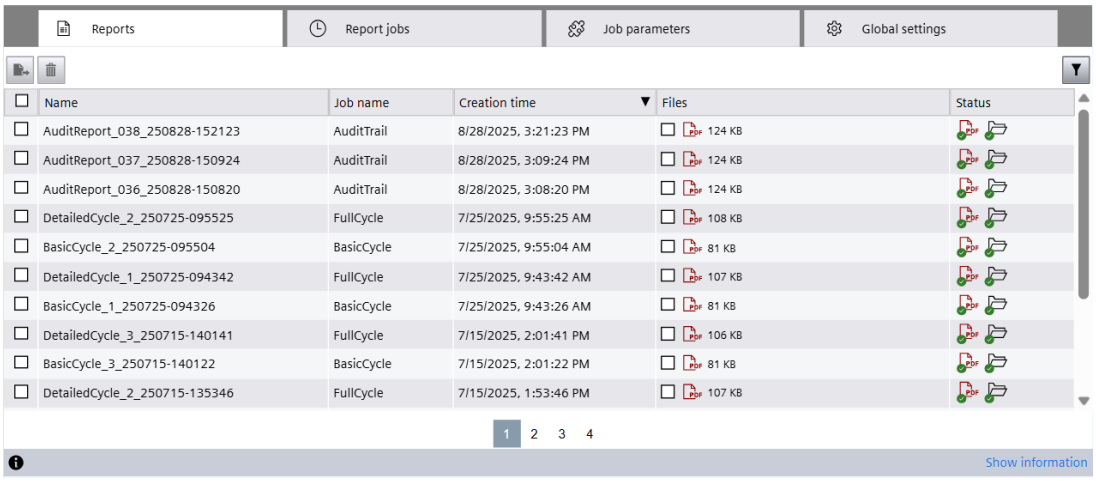

Figure 4: Reports management in WinCC Unified

Appendix 2

SIMATIC WinCC Unified Electronic Signature

Introduction

In the realm of electronic records and electronic signatures (ERES), SIMATIC WinCC Unified V20 offers robust solutions tailored to meet regulatory requirements. The electronic signature functionality within WinCC Unified ensures that electronic records are as reliable and trustworthy as paper records and handwritten signatures executed on paper.

Electronic signature functionality

Simple electronic signature

The configuration of an electronic signature is available with the WinCC Unified Audit option (Basic or Enhanced). The electronic signature is executed in a dialog where users confirm the intended action by entering their password. The variables requiring an electronic signature in the case of changes are specified during the configuration phase. Users can sign electronically by confirming the intended action, and the electronic signature is saved in the audit trail along with the user name, time stamp, and the action performed. The mandatory entry of a comment can be selected.

Multiple electronic signature

With the WinCC Unified Audit Enhanced variant, a double electronic signature can also be configured, ensuring an extra layer of validation and security.

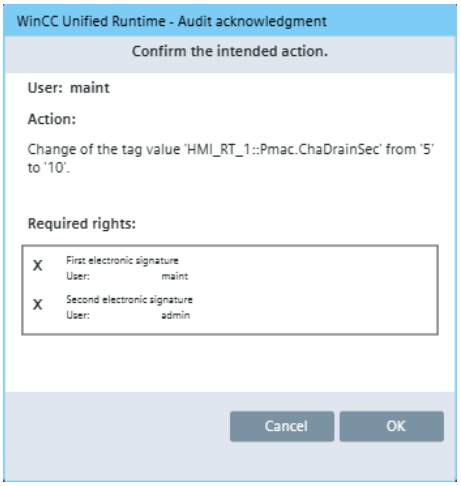

Figure 5: Double signature screen in WinCC Unified

Ensuring uniqueness and integrity

The electronic signature within WinCC Unified is designed to be unique to each individual, preventing the reuse or reassignment of signatures. It is linked to its respective electronic record to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify the electronic record by ordinary means.

Regulatory compliance

The electronic signature feature meets the requirements of 21 CFR Part 11 and Annex 11 of the EU-GMP Guidelines. This regulatory compliance ensures that the electronic signatures are legally binding and equivalent to hand-written signatures executed on paper. The system also supports the ability to generate accurate and complete copies of electronic records, including the electronic signature details, in both human-readable and electronic form.

Conclusion

The electronic signature functionality in WinCC Unified provides a secure and compliant environment for recording and verifying electronic signatures in GMP-relevant processes. It ensures data integrity, authenticity, and traceability, making it an essential component for regulatory compliance in the life science industry.

GETINGE

With a firm belief that every person and community should have access to the best possible care, Getinge provides hospitals and life science institutions with products and solutions aiming to improve clinical results and optimize workflows. The offering includes products and solutions for intensive care, cardiovascular procedures, operating rooms, sterile reprocessing and life science. Getinge employs over 10,000 people worldwide and the products are sold in more than 135 countries.

Ekebergsvägen 26 · Box 69 · SE-305 05 Getinge · Sweden

www.getinge.com