SIEMENS

Edition

08/2023

COMPLIANCE RESPONSE ERES

SIMATIC

WinCC Comfort/Advanced V17/V18

Electronic Records / Electronic Signatures

siemens.com/pharma

SIEMENS

SIMATIC

WinCC Comfort/Advanced V17/V18 ERES Compliance Response

Product Information

Electronic Records /
Electronic Signatures (ERES)

08/2023
A5E52702640-AA

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

⚠ DANGER

indicates that death or severe personal injury **will** result if proper precautions are not taken.

⚠ WARNING

indicates that death or severe personal injury **may** result if proper precautions are not taken.

⚠ CAUTION

indicates that minor personal injury can result if proper precautions are not taken.

NOTICE

indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

⚠ WARNING

Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E52702640-AA
Ⓟ 08/2023 Subject to change

Table of contents

Introduction

1

Life science industry is basing key decisions on regulated records that are increasingly generated, processed and kept electronically. Reviews and approval of such data are also being provided electronically. Thus the appropriate management of electronic records and electronic signatures has become an important topic for the life science industry.

Accordingly, regulatory bodies defined criteria under which electronic records and electronic signatures will be considered as reliable and trustworthy as paper records and handwritten signatures executed on paper. These requirements have been set forth by the US FDA in 21 CFR Part 11 (21 CFR Part 11 Electronic Records; Electronic Signatures, US FDA, 1997; in short: *Part 11*) and by the European Commission in Annex 11 of the EU GMP Guideline (EU Guidelines to Good Manufacturing Practice, Volume 4, Annex 11: Computerised Systems, European Commission, 2011; in short: *Annex 11*).
Since requirements on electronic records and electronic signatures are always tied to a computerized system being in a validated state, both regulations also include stipulations on validation and lifecycle of the computerized system.

Application of *Part 11* and *Annex 11* (or their corresponding implementation in national legislation) is mandatory for the use of electronic records and electronic signatures. However, these regulations are only valid within their defined scope.
The scope of both regulations is defined by the regional market to which the finished pharmaceutical product is distributed and by whether or not the computerized systems and electronic records are used as part of GMP-regulated activities (see Part 11.1 and Annex 11 Principle).

Supplemental to the regulations, a number of guidance documents, good practice guides and interpretations have been published in recent years to support the implementation of the regulations. Some of them are referred to within this document.

To help its clients, Siemens as supplier of SIMATIC WinCC (TIA Portal) has evaluated the system with regard to these requirements and published its results in this Compliance Response. Since version 18 is not available for Comfort Panels and Runtime Advanced, the device version V17 continues to be used in WinCC (TIA Portal) V18 Engineering. This document therefore references V17/V18.

SIMATIC WinCC Comfort/Advanced V17/V18 fully meets the functional requirements for the use of electronic records and electronic signatures.

Operation in conformity with the regulations is ensured in conjunction with organizational measures and procedural controls to be established by the regulated user. Such measures and controls are mentioned in chapter "Evaluation List for WinCC Comfort/Advanced (Page 17)" of this document.

This document is divided into three parts:

1. Chapter "The Requirements in Short (Page 7)" provides a brief description of the requirement topics.
2. Chapter "Meeting the Requirements with WinCC Comfort/Advanced (Page 9)" introduces the functionality of the system with which these requirements are met.
3. Chapter "Evaluation List for WinCC Comfort/Advanced (Page 17)" contains a detailed system assessment on the basis of the individual requirements of the relevant regulations.

The Requirements in Short

2

The requirements of Annex 11 and Part 11 have the purpose of protecting regulated electronic records and electronic signatures (short: ERES) against manipulation, misinterpretations and incomprehensible changes.

The term "electronic record" means any combination of text, graphics, data, audio, pictorial or other information representation in digital form, that is created, modified, maintained, archived, retrieved or distributed by a computer system for use in a regulated process.

The "electronic signature" is a legally binding equivalent of a handwritten signature. The submission of the signature is a technical process for identifying the signatory, whereas the representation of the signature in connection with the signed action becomes part of the electronic documentation. Since electronic signatures are also considered as being electronic records by themselves, all requirements for electronic records are applied to electronic signatures too.

The following table provides an overview of the requirements from both regulations.

Requirement	Description
Lifecycle and Validation of Computerized Systems	Computerized systems used as a part of GMP-related activities must be validated. The validation process should be defined using a risk-based approach. It should cover all relevant steps of the lifecycle and must provide appropriate documented evidence. The system's functionality should be traceable throughout the lifecycle by being documented in specifications or a system description. A formal change control procedure as well as an incident management should be established. Periodic evaluation should confirm that the validated state of the system is being maintained.
Suppliers and Service Providers	Since competency and reliability of suppliers and service providers are considered key factors, the supplier assessment should be decided on a risk-based approach. Formal agreements should exist between the regulated user and these third parties, including clear responsibilities of the third party.
Data Integrity	Under the requirements of both regulations, electronic records and electronic signatures must be as reliable and trustworthy as paper records. The system must provide the ability to discern altered records. Built-in checks for the correct and secure handling of data should be provided for manually entered data as well as for data being electronically exchanged with other systems. The system's ability to generate accurate and complete copies is essential for the use of the electronic records for regulated purposes, as well as the accessibility, readability, and integrity of archived data throughout the retention period.
Audit Trail, Change Control Support	Besides recording changes to the system as defined in the lifecycle, both regulations require that changes on GMP-relevant data are being recorded. Such an audit trail should include information on the change (before / after data), the identity of the operator, a time stamp, as well as the reason for the change.

Requirement	Description
System Access, Identification Codes and Passwords	Access to the system must be limited to authorized individuals. Attention should be paid to password security. Changes on the configuration of user access management should be recorded. Periodic reviews should ensure the validity of identification codes. Procedures should exist for recalling access rights if a person leaves and for loss management. Special consideration should be given to the use of devices that bear or generate identification code or password information.
Electronic Signature	Regulations consider electronic signatures being legally binding and generally equivalent to handwritten signatures executed on paper. Beyond requirements on identification codes and passwords as stated above, electronic signatures must be unique to an individual. They must be linked to their respective electronic record and not be copied or otherwise being altered.
Open Systems	Open systems might require additional controls or measures to ensure data integrity and confidentiality.

Meeting the Requirements with WinCC Comfort/ Advanced

3

The Siemens recommendations for the system architecture, conception, and configuration will assist system users in achieving compliance. More information and help is available in the "System Manual SIMATIC STEP 7 and WinCC Engineering (TIA Portal)" (see Online Support under entry ID 109815056).

The requirements explained in chapter "The Requirements in Short (Page 7)" can be supported by the system as follows.

The basic data control policies of a regulated company relate to persons, processes and techniques.

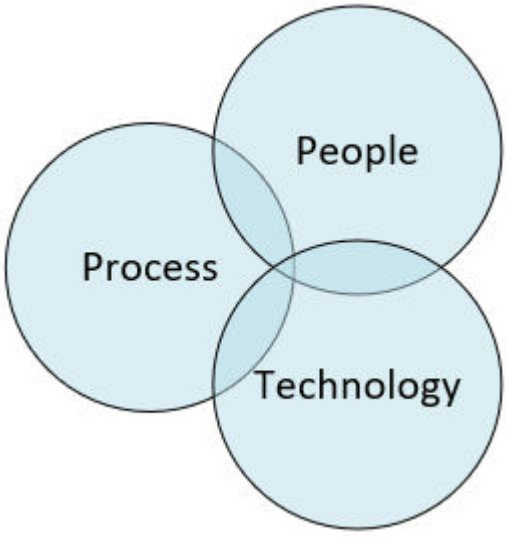

Figure 3-1 Elements of data control

Only the sum of all measures can ensure that the system is operated in compliance with the regulatory requirements.

- Process: Procedures, for example, for operation, change management, validation and archiving
- People: Suitable qualification, training of staff and following the established processes
- Technology: Selection and functionality of the basic components as well as specific configuration for the application

3.1 Lifecycle and Validation of Computerized Systems

In Annex 11 from 1992 and in Part 11 from 1997, the law already required that computerized systems need to be validated. Criteria for the validation of the system and its lifecycle were added in the edited revision of Annex 11 from 2011.

Requirements for the validation of computerized systems and for the maintenance of the validated state are also part of other publications, such as the Baseline Guides, the GAMP Guides and the GAMP Good Practice Guides of the ISPE (International Society of Pharmaceutical Engineers (https://www.ispe.org)) industry association.

Consequently, the system lifecycle and validation approach should be defined taking into account the recommendations of the GAMP 5 Guide (GAMP 5 - A risk-based approach to compliant GxP computerized systems). Topics such as lifecycle management, system development and operation of computerized systems are also dealt with in detail in the GAMP Guides.

3.2 Suppliers and Service Providers

Suppliers of systems, solutions and services must be evaluated accordingly, see GAMP 5 Appendix M2. Siemens as a manufacturer of hardware and software components follows internal procedures of Product Lifecycle Management and works according to a Quality Management System, which is regularly reviewed and certified by an external certification company.

3.3 Data Integrity

Regulated companies should implement integrated data integrity strategies. Of particular interest are the data used to make decisions that have an impact on product quality and patient safety.

The reliability of the data requires a high degree of data integrity over the entire retention period and also extends to the archiving and retrieval of data.

In addition, the system must have the ability to detect invalid or altered records. On the computer system side, functionalities such as access protection, audit trail, data type checks, checksums, data backup/restore, and data archiving/retrieval help maintain data integrity. These measures and technical characteristics are complemented by system validation, appropriate work procedures and staff training.

IT security

IT Security is also essential for achieving and retaining data integrity. Support from Siemens can be found under Industrial Security Services. (https://new.siemens.com/global/en/products/services/digital-enterprise-services/industrial-security-services.html)

Continuous recording and logging

Process data (messages, process values) and audit trails can be recorded and stored. It can also be transferred into long-term archives.

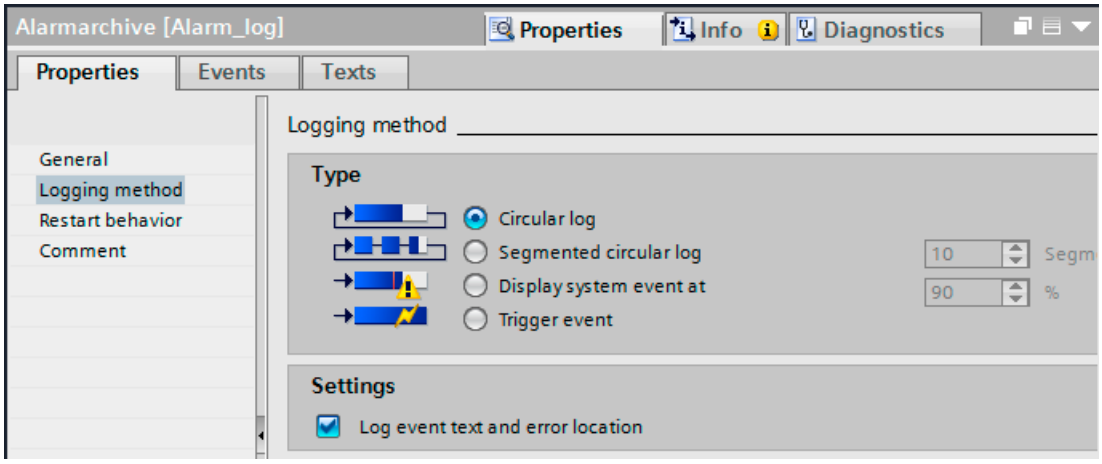

Figure 3-2 Configuration of archiving strategy

In the case of local HMI panels, the data are buffered on a local storage device (e.g. SD card), and then transferred via the network or a USB device.

Batch-oriented archiving

The WinCC premium add-on, PM-QUALITY, is used for batch-oriented data archiving. PM-QUALITY automatically manages the local and long-term archives. To enable access to WinCC data, PM-QUALITY deploys the interfaces of SIMATIC WinCC. Such interfaces are also available for other archiving tools (Siemens or third-party manufacturers).

3.4 Audit Trail, Change Control Support

"Audit trails are of particular importance in areas where operator actions generate, modify, or delete data in the course of normal operation." (Guidance for Industry Part 11 – Scope and Application, FDA, 2003)

An audit trail is not required for automatically generated electronic records which can neither be modified nor deleted by the operator. The system provides adequate system security mechanisms for such electronic records.

Changes to the configuration of a validated system are subject to a change procedure and must be controlled accordingly. This can be supported by versioning, system logs and similar means. The following sections therefore distinguish between the requirements for audit trails during operation and the control of configuration changes in engineering.

Operator inputs / recordings during operation

SIMATIC WinCC Comfort/Advanced 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.

The GMP relevant data is defined by the regulated user based on the applicable regulatory requirements.

Recording process data

Process data (e.g. process values, messages and alarms) is stored in the system, without any option for the operator to change this data. No audit trail is required for this data.

Operator input during operation

All modifications and inputs of relevant data, which the operator makes during operation, are logged in an audit trail. The relevant data to be tracked in the audit trail can be configured on the engineering system, see figure below. When performing this, you can select "Acknowledgment", "without acknowledgment" or "with electronic signature" as confirmation type. A comment can be optional or mandatory.

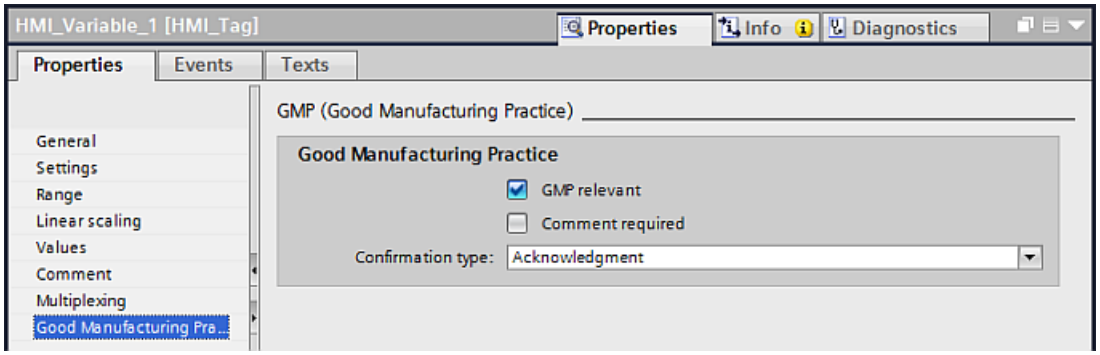

Figure 3-3 Marking a GMP-relevant variable for the audit trail

The audit trail can be saved and archived as a separate file. An integrated algorithm automatically forms a checksum for each record.

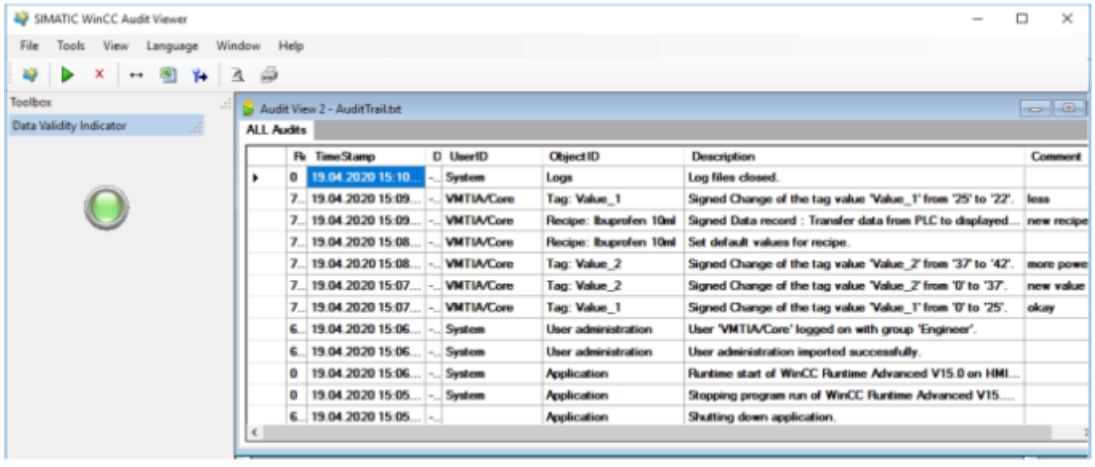

Figure 3-4 Audit Viewer

The Audit Viewer displays the audit trail file from Comfort Panels and WinCC Runtime Advanced and confirms with the green signal lamp that the audit trail has not been manipulated.

Configuration control

In contrast to the audit trail, changes to the system configuration are subject to the procedure of change control. Before they are executed, such changes are planned, their potential effects are assessed, documented during the execution and finally tested for correct implementation. The documentation of the changes made can be supported by various tools.

SIMATIC WinCC (TIA Portal) provides system functions, options, and add-ons to support the control of the system configuration. This includes versioning of software elements and projects as well as backup/restore functions to support the corresponding procedures. For more details, see "GMP Engineering Manual SIMATIC WinCC (TIA Portal)" from Siemens.

3.5 System Access, Identification Codes and Passwords

Users must be assigned the required access rights only, in order to prevent unauthorized access to and unintended manipulation of the file system, directory structures, and system data.

The requirements regarding access security are fully met in combination with procedural controls, such as those for "specifying rights and roles".

Adequate security mechanisms are essential for the secure operation of a system. This applies especially to "open paths" which must be protected by additional measures. For more information on the basic policies of the security concept and configuration recommendations, refer to the "Security Concept PCS 7 and WinCC" manual (see Online Support under entry ID 109780811).

The user administration configuration is performed centrally on an engineering system for each application. After the login data is checked for correctness, the corresponding user group information which determined the user access rights is transferred to the respective HMI devices.

SIMATIC WinCC (TIA Portal) supports the protection of electronic records by providing:

- Usage of a unique identification code
- Definition of access authorizations for user groups/roles
- Password settings and password aging
- Blocking a user after a configurable number of failed login attempts

Centralized user administration

When an HMI device is operated in a network, central user management offers significant advantages. It is based on Microsoft Windows and SIMATIC Logon, if applicable in a domain structure.

- Individual users and their assignment to Windows user groups are defined in the User Account Control of Microsoft Windows.
- SIMATIC Logon provides the link between the Windows user groups and the user groups of the WinCC Runtime system.

- Based on user groups, user rights with different levels are defined in the user administration for the particular HMI device or WinCC Runtime system.
- If the network connection fails, user administration is taken over by the local user administration. This allows a predefined local emergency user to be used for predefined emergency operation. SIMATIC Logon users (central users) that are already logged on remain active until logoff.

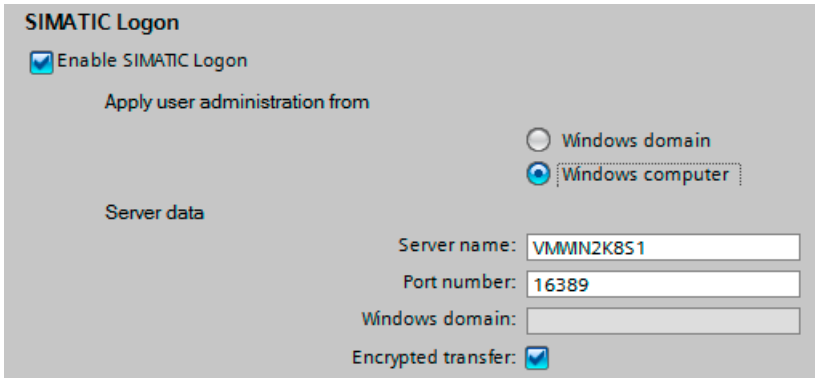

Figure 3-5 Enable user administration based on Microsoft Windows and SIMATIC Logon for a Comfort Panel or WinCC RT Advanced

User administration on local HMI devices

Local HMI panels are quite often installed without any connection to a network. Therefore, in SIMATIC WinCC (TIA Portal), local user administration can be implemented on these HMI devices. Individual users and their assignment to user groups are then only known locally.

- Individual users and their assignment to user groups are defined in the WinCC configuration.
- Based on user groups, user rights with different levels are defined in the user administration for the particular HMI device or WinCC Runtime Advanced system.

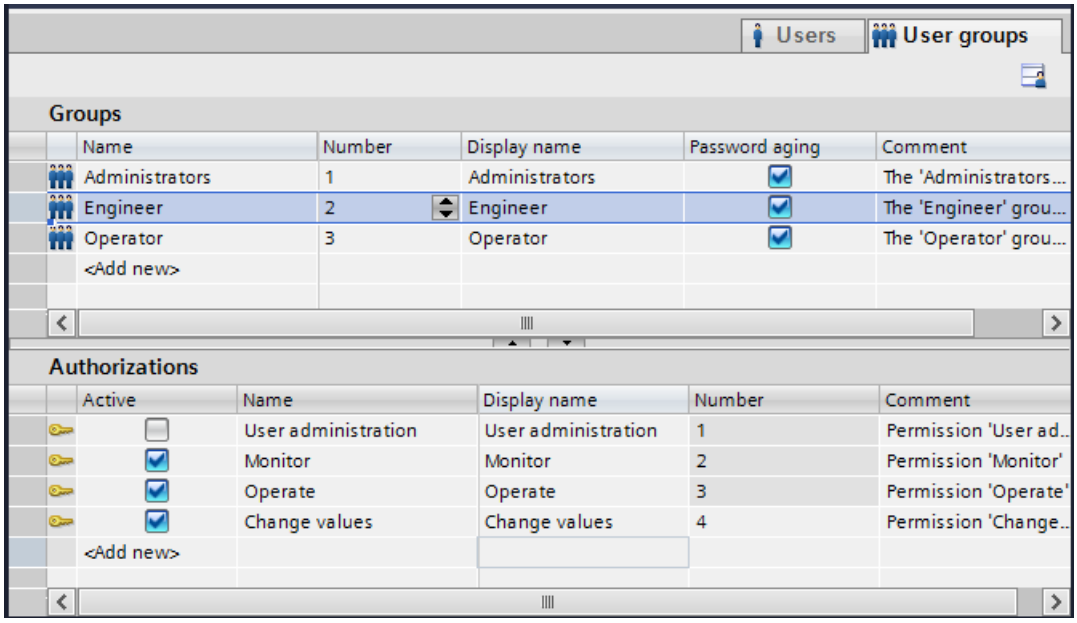

Figure 3-6 Assignment of user rights to user groups

3.6 Electronic Signature

SIMATIC WinCC (TIA Portal) provides functions for configuring an electronic signature. The electronic signature is executed in a dialog. Which variables may require an electronic signature upon changes is specified during the configuration phase. Users can sign electronically by confirming the intended action by entering their password. In this way, the electronic signature is saved in the audit trail along with the user name, time stamp, and the action performed.

With the options "SIMATIC WinCC Audit for SIMATIC Panels" or "SIMATIC WinCC Audit for Runtime Advanced", a separate signature dialog is available for SIMATIC Comfort Panels or WinCC Runtime Advanced. The comment can be configured as optional or mandatory for each object.

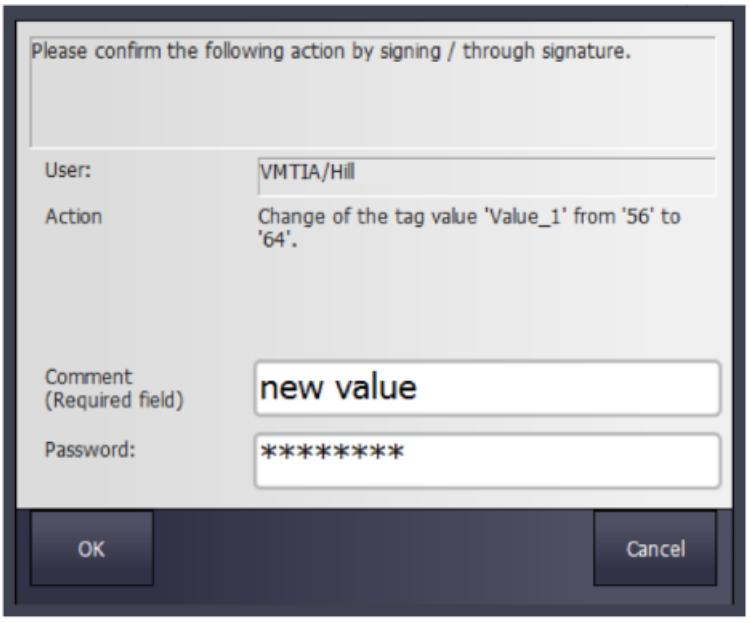

Figure 3-7 Electronic signature with comment for modification of a tag value via a Comfort Panel or in WinCC Runtime Advanced

Evaluation List for WinCC Comfort/Advanced

4

The following list of requirements includes all regulatory requirements from 21 CFR Part 11 as well as from Annex 11 of the EU-GMP Guidelines. All requirements are structured in the same topics as those introduced in the chapter "The Requirements in Short (Page 7)" of this Compliance Response.

The *requirements* listed fully consider both regulations, regardless of whether technological or procedural controls or a combination of both are needed to fully comply with Part 11 and Annex 11.

The *answers* include, among other things, information about how the requirement is handled during the development of the product and which measures should be implemented during configuration and operation of the system. Furthermore, the answers include references to the product documentation for technical topics and to the GAMP 5 guide for procedural controls that are already considered in the guide.

4.1 Lifecycle and Validation of Computerized Systems

The fundamental requirement that a computerized system, used as a part of GMP related activities, must be validated is extended in the revision of Annex 11 from 2011 by requirements detailing expectations on a system's lifecycle.

	Requirement	Reference	Answer
4.1.1	Risk management should be applied throughout the lifecycle of the computerized system.	Annex 11, 1	Yes. The PLM (Product Lifecycle Management) process is the development process for Siemens software products. This process includes appropriate risk management. During the validation and operation of a system, risk management should be ensured by the regulated user.
4.1.2	Validation of a system ensures its accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	21 CFR 11.10 (a)	Yes. The development of the software product (COTS, see Annex 11, Glossary) is subject to the Siemens QMS and the PLM process. The regulated user should take appropriate measures to validate the application (see Annex 11, glossary), as well as maintaining its validated state.
4.1.3	Validation documentation covers all relevant steps of the lifecycle.	Annex 11, 4.1	Yes. The PLM process contains all relevant documents. The responsibility for the validation of the application (see Annex 11, glossary) is with the regulated user.
4.1.4	A process for the validation of bespoke or customized systems should be in place.	Annex 11, 4.6	Customer-specific applications are verified in the scope of realization according to the responsibilities agreed upon in the project. The validation process is the responsibility of the regulated user.

	Requirement	Reference	Answer
4.1.5	Change management and deviation management are applied during the validation process.	Annex 11, 4.2	Yes. The PLM process includes procedures for managing changes and deviations as well as error corrections. The regulated user should ensure appropriate change management and deviation management (see GAMP 5, appendices M8 and D5).
4.1.6	An up-to-date inventory of all relevant systems and their GMP functionality is available. For critical systems, an up-to-date system description [...] should be available.	Annex 11, 4.3	The regulated user should establish appropriate reporting, a system inventory as well as system descriptions (see GAMP 5, appendix D6).
4.1.7	User Requirements Specifications (URS) should describe the required functions. They must also follow a risk-based approach and be traceable throughout the entire lifecycle.	Annex 11, 4.4	Yes. Specification of requirements is part of the PLM process. For project-specific configuration, the regulated user must describe the user requirements in the lifecycle of the system (see GAMP 5, appendix D1).
4.1.8	Evidence of appropriate test methods and test scenarios should be demonstrated.	Annex 11, 4.7	Ensuring the suitability of test methods and scenarios is an integral part of the PLM process and test planning. The regulated user should be involved in or agree to the testing practice (see GAMP 5, appendix D5) for the application.
4.1.9	Appropriate controls should be used over system documentation. Such controls include the distribution of, access to, and use of system operation and maintenance documentation.	21 CFR 11.10 (k)	During the development of the product, the product documentation is treated as part of the product. Thus, the documentation itself is also subject to the requirements of the PLM process. The regulated user should establish appropriate procedural controls during development and operation of a productive system (see GAMP 5, appendices M9 and D6).
4.1.10	A formal change control procedure for system documentation maintains a time-sequenced record of changes.	21 CFR 11.10 (k) Annex 11.10	During the development of the product, changes are handled according to the PLM process. The regulated user should establish appropriate procedural controls during development and operation of the system (see GAMP 5, appendices M8 and O6).
4.1.11	Persons, who develop, maintain, or use electronic record/ electronic signature systems should have the education, training and experience to perform their assigned task.	21 CFR 11.10 (i)	Siemens' processes ensure that employees have appropriate training for their tasks and that such training is properly documented. Furthermore, Siemens offers a variety of training courses for users, administrators and support staff.
4.1.12	Computerized systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP.	Annex 11, 11	The regulated user should establish appropriate procedural controls (see GAMP 5, appendices O3 and O8).

	Requirement	Reference	Answer
4.1.13	All incidents should be reported and assessed.	Annex 11, 13	The SIMATIC portfolio offers functionalities to support reporting on different system levels. The regulated user should establish appropriate procedural controls (see GAMP 5, appendix O5).
4.1.14	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.	Annex 11, 16	The regulated user should appropriately consider the system in their business continuity plan (see GAMP 5, appendix O10).

4.2 Suppliers and Service Providers

If the regulated user is partnering with third parties for planning, development, validation, operation and maintenance of a computerized system, then the competence and reliability of this partner should be considered utilizing a risk-based approach.

	Requirement	Reference	Answer
4.2.1	When third parties are used, formal agreements must exist between the manufacturer and any third parties.	Annex 11, 3.1	The regulated user is responsible for establishing formal agreements with suppliers and third parties (see GAMP 5, appendix O2).
4.2.2	The competency and reliability of a supplier are key factors when selecting a product or service provider. The need for an audit should be based on a risk assessment.	Annex 11, 3.2 Annex 11, 4.5	The regulated user should assess its suppliers accordingly (see GAMP 5, appendix M2).
4.2.3	The regulated user should ensure that the system has been developed in accordance with an appropriate quality management system.	Annex 11, 4.5	The development of SIMATIC products follows the PLM process stipulated in Siemens' Quality Management System.
4.2.4	Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to verify that user requirements are fulfilled.	Annex 11, 3.3	The regulated user is responsible for the performance of such reviews.
4.2.5	Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request.	Annex 11, 3.4	The content and extent of the documentation affected by this requirement should be agreed upon by the regulated user and Siemens. The joint non-disclosure agreement should reflect this requirement accordingly.

4.3 Data Integrity

The main goal of both regulations is to define criteria under which electronic records and electronic signatures are as reliable and trustworthy as paper records. This requires a high degree of data integrity throughout the whole data retention period, including archiving and retrieval of relevant data.

	Requirement	Reference	Answer
4.3.1	The system should provide the ability to discern invalid or altered records.	21 CFR 11.10 (a)	This is made feasible with the following functions: time stamping, revisions, versioning for configuration and documents, and audit trail for operational entries.
4.3.2	For records supporting batch release, it should be possible to generate printouts indicating if any of the data has been changed since the original entry.	Annex 11, 8.2	Operational modification of data is recorded in the general audit trail and can be printed in a report with internal or add-on functions.
4.3.3	The system should provide the ability to generate accurate and complete copies of electronic records in both human readable and electronic form.	21 CFR 11.10 (b) Annex 11, 8.1	Yes. Accurate and complete copies can be generated in electronic format or on paper.
4.3.4	Computerized systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data.	Annex 11, 5	Yes. Depending on the type of data, such built-in checks include data type checks, access authorizations, checksums, etc. and finally the validation process including interface testing.
4.3.5	For critical data entered manually, there should be an additional check on the accuracy of the data.	Annex 11, 6	The system has built-in plausibility checks for data entry. In addition, an operator dialog can be realized as an additional check.
4.3.6	Data should be secured by both physical and electronic means against damage.	Annex 11, 7.1	In addition to the system's access security mechanisms, the regulated user should establish appropriate security means such as physical access control, backup strategy, limited user access authorizations, regular checks on data readability, etc. Furthermore, the data retention period should be determined by the regulated user and appropriately considered in the user's processes (see GAMP 5, appendices O3, O4, O8, O9, O11, O13).
4.3.7	Regular back-ups of all relevant data should be done.	Annex 11, 7.2	The regulated user must establish appropriate processes for data backup and restore (see GAMP 5, appendix O9).
4.3.8	Electronic records must be readily retrievable throughout the records retention period.	21 CFR 11.10 (c) Annex 11, 17	Yes. When exporting archives, the regulated user must establish procedural controls for archiving and retrieval of data (see GAMP 5, Appendix O13).
4.3.9	If the sequence of system steps or events is important, then appropriate operational system checks should be enforced.	21 CFR 11.10 (f)	Yes. A specific sequence of operator actions can be provided by configuring the application accordingly, for example.

4.4 Audit Trail, Change Control Support

During operation, regulations require the recording of operator actions that may result in the generation of new relevant records or the alteration or deletion of existing records.

	Requirement	Reference	Answer
4.4.1	The system should create 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.	21 CFR 11.10 (e) Annex 11, 9	Yes. Changes during operation can be traced back by the system itself via an audit trail and contain information with time stamp, user ID, old and new value, as well as comments. The audit trail is secure within the system and cannot be changed by a user.
4.4.2	Management systems for data and documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time.	Annex 11, 12.4	Yes. Operator interventions are recorded with identification code and time stamp.
4.4.3	Changes to electronic records shall not obscure previously recorded information.	21 CFR 11.10 (e)	Yes. Recorded information is not overwritten and is always available in the database.
4.4.4	The audit trail shall be retained for a period at least as long as that required for the subject electronic records.	21 CFR 11.10 (e) Annex 11, 9	Yes. This is technically feasible and must be considered in the application-specific backup and restore process (see GAMP 5, appendices O9 and O13).
4.4.5	The audit trail shall be available for review and copying by regulatory agencies.	21 CFR 11.10 (e)	Yes, see also requirement 4.4.1.

4.5 System Access, Identification Codes and Passwords

Since access to a system must be restricted to authorized individuals and the uniqueness of electronic signatures also depends on the authenticity of user credentials, user access management is a vital set of requirements regarding the acceptance of electronic records and electronic signatures.

	Requirement	Reference	Answer
4.5.1	System access should be limited to authorized individuals.	21 CFR 11.10 (d) 21 CFR 11.10 (g) Annex 11, 12.1	Yes. System access can be managed via the user administration. The single user rights must be specified by the regulated user. Procedural controls should also be established by the regulated user, as described in GAMP 5, appendix O11.
4.5.2	The extent of security controls depends on the criticality of the computerized system.	Annex 11, 12.2	System security is a key factor during design and development of SIMATIC products. Since system security strongly depends on the operating environment of the specific IT system, these aspects should be considered in security management (see GAMP 5, appendix O11). Recommendations and support are available from Siemens Industrial Security.
4.5.3	Creation, change, and cancellation of access authorizations should be recorded.	Annex 11, 12.3	Changes in the user access management are recorded and should be subject to the change control procedure of the regulated user.

	Requirement	Reference	Answer
4.5.4	If it is a requirement of the system that input data or instructions can only come from certain input devices (e.g. terminals), does the system check the validity of the source of any data or instructions received? (Note: This applies where data or instructions can come from more than one device, and therefore the system must verify the integrity of its source, such as a network of weigh scales, or remote, radio-controlled terminals).	21 CFR 11.10 (h)	Yes. The WinCC HMI devices can be configured so that special input data/commands can only be performed from a dedicated device, or from a group of dedicated devices. All other devices then have read-only access rights at the most.
4.5.5	Controls should be in place to maintain the uniqueness of each combined identification code and password, so that no individual can have the same combination of identification code and password as any other.	21 CFR 11.300 (a)	Yes. It is ensured that every identification code is unique within the system. Every combination of identification code and password is therefore also unique.
4.5.6	Procedures are in place to ensure that the validity of identification codes is periodically checked.	21 CFR 11.300 (b) Annex 11, 11	The regulated user must establish appropriate procedural controls.
4.5.7	Password should periodically expire and have to be revised.	21 CFR 11.300 (b)	Yes. Password aging can be configured in the user administration.
4.5.8	A procedure should be established for recalling identification codes and passwords if a person leaves or is transferred.	21 CFR 11.300 (b) Annex 11, 12.1	Yes. A user account can be disabled or the assigned access rights can be withdrawn for that user. The regulated user must establish appropriate procedural controls.
4.5.9	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.	21 CFR 11.300 (c)	The regulated user must establish appropriate procedural controls.

	Requirement	Reference	Answer
4.5.10	Measures for detecting attempted unauthorized use and for informing security and management should be in place.	21 CFR 11.300 (d) Annex 11, 12.1	Yes. Unsuccessful attempts to use the system or to perform electronic signatures are recognized and can be logged. The regulated user should establish appropriate procedural controls to ensure a periodic review of security and access control information logs (see GAMP 5, appendix O8).
4.5.11	Initial and periodic testing of devices, such as tokens and 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.	21 CFR 11.300 (e)	Such devices are not part of the SIMATIC HMI portfolio, but may be integrated in the system via SIMATIC Logon. The regulated user must establish appropriate procedural controls.

4.6 Electronic Signature

To ensure that electronic signatures are generally accepted as equivalent to handwritten signatures executed on paper, requirements are not only limited to the act of electronically signing records. They also include requirements on record keeping as well as on the manifestation of the electronic signature.

	Requirement	Reference	Answer
4.6.1	Written policies should be established, that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	21 CFR 11.10 (j) Annex 11, 14.a	The regulated user should establish appropriate procedural controls.
4.6.2	Signed electronic records should contain the following related information: • The printed name of the signer • The date and time of signing • The meaning of the signing (such as approval, review, responsibility)	21 CFR 11.50 (a) Annex 11, 14.c	Yes.
4.6.3	The above listed information is shown on displayed and printed copies of the electronic record.	21 CFR 11.50 (b)	Yes.
4.6.4	Electronic signatures 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.	21 CFR 11.70 Annex 11, 14.b	Yes.

	Requirement	Reference	Answer
4.6.5	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	21 CFR 11.100 (a) 21 CFR 11.200 (a) (2)	Yes. The electronic signature uses the unique identifiers for user accounts. The re-use or re-assignment of electronic signatures is effectively prevented.
4.6.6	When a 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 batch.	Annex 11, 15	Electronic signatures are linked to an individual. The system allows strict determinations of which role and/or individual is allowed to perform a signature.
4.6.7	The identity of an individual should be verified before electronic signature components are allocated.	21 CFR 11.100 (b)	The regulated user should establish appropriate procedural controls for the verification of an individual's identity before allocating a user account and/or electronic signatures.
4.6.8	When an individual executes one or more signings not performed during a single session, each signing shall be executed using all of the electronic signature components.	21 CFR 11.200 (a) (1) (ii)	Yes. Performing an electronic signature requires the user ID as well as the user's password.
4.6.9	When an individual executes a series of signings during a single session, the first signing shall be executed using all electronic signature components. Subsequent signings shall be executed using at least one private electronic signature component.	21 CFR 11.200 (a) (1) (i)	Yes. Each signature consists of two components (user ID and password).
4.6.10	The use of an individual's electronic signature by anyone other than the genuine owner would require the collaboration of two or more individuals.	21 CFR 11.200 (a) (3)	Yes. 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.
4.6.11	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owner.	21 CFR 11.200 (b)	Standard tools of third-party manufacturers can be used to create biometric electronic signatures. The integrity of such solutions should be assessed separately.

4.7 Open Systems

The operation of an open system may require additional controls to ensure data integrity as well as the possible confidentiality of electronic records.

	Requirement	Reference	Answer
4.7.1	To ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records additional measures such as data encryption are used.	21 CFR 11.30	Additional security measures should be taken for open systems. For example, support is provided with configuration information in the "Security Concept PCS 7 and WinCC" manual, or by commonly available standard tools for encryption.
4.7.2	To ensure the authenticity and integrity of electronic signatures, additional measures such as the use of digital signature standards are used.	21 CFR 11.30	SIMATIC WinCC (TIA Portal) does not provide functionality for digital (encrypted) signatures.

Get more information

Siemens AG
Digital Industries
Pharmaceutical and Life Science Industry
Siemensallee 84
76187 Karlsruhe, Germany

PDF (A5E52702640-AA)
Produced in Germany