



SIEMENS

Edition

09/2023

COMPLIANCE RESPONSE ERES

SIMATIC

SIMATIC WinCC V8.0

Electronic Records / Electronic Signatures

[siemens.com/pharma](https://www.siemens.com/pharma)

SIEMENS

SIMATIC

SIMATIC WinCC V8.0 ERES Compliance Response

Product Information

Electronic Records /
Electronic Signatures (ERES)

Introduction

1

The Requirements in Short

2

Meeting the Requirements
with SIMATIC WinCC

3

Evaluation List for SIMATIC
WinCC

4

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.

Table of contents

1	Introduction	5
2	The Requirements in Short	7
3	Meeting the Requirements with SIMATIC WinCC	9
3.1	Lifecycle and Validation of Computerized Systems	10
3.2	Suppliers and Service Providers	10
3.3	Data Integrity	10
3.4	Audit Trail, Change Control Support	11
3.5	System Access, Identification Codes and Passwords	13
3.6	Electronic Signature	14
4	Evaluation List for SIMATIC WinCC	17
4.1	Lifecycle and Validation of Computerized Systems	17
4.2	Suppliers and Service Providers	19
4.3	Data Integrity	19
4.4	Audit Trail, Change Control Support	20
4.5	System Access, Identification Codes and Passwords	21
4.6	Electronic Signature	23
4.7	Open Systems	24

Introduction

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 customers, Siemens as the supplier of SIMATIC WinCC, has evaluated the system with regard to these requirements and the results are published in this Compliance Response.

SIMATIC WinCC V8.0 is compliant with all 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 SIMATIC WinCC (Page 17)" of this document.

This document is divided into three parts:

1. The chapter "The Requirements in Short (Page 7)" provides a brief description of the requirement clusters.
2. Chapter "Meeting the Requirements with SIMATIC WinCC (Page 9)" introduces the functionality of SIMATIC WinCC as means to meet those requirements.
3. Chapter "Evaluation List for SIMATIC WinCC (Page 17)" contains a detailed system assessment on the basis of the individual requirements of the relevant regulations.

The Requirements in Short

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 SIMATIC WinCC

The Siemens recommendations for the system architecture, conception, and configuration will assist system users in achieving compliance. For additional information and assistance, refer to "GMP Engineering Manual SIMATIC WinCC" from Siemens.

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.

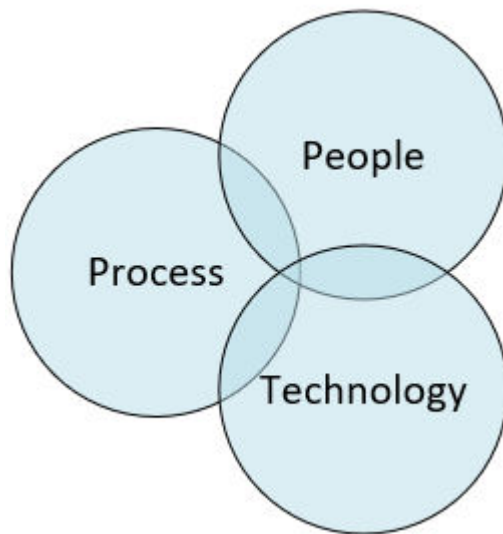


Figure 3-1 Elements of data control

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

3.3 Data Integrity

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 archiving

SIMATIC WinCC provides a configurable and scalable archiving concept. Messages and measured values are stored continuously to local WinCC archives. This locally stored data can be transferred automatically to long-term archives. Generation of checksums detects any manipulation of the archived data. Archived data can be retrieved within the entire, configured retention period. The data can be called in SIMATIC WinCC either by using standard functions or additional interfaces such as DataMonitor or Connectivity Pack.

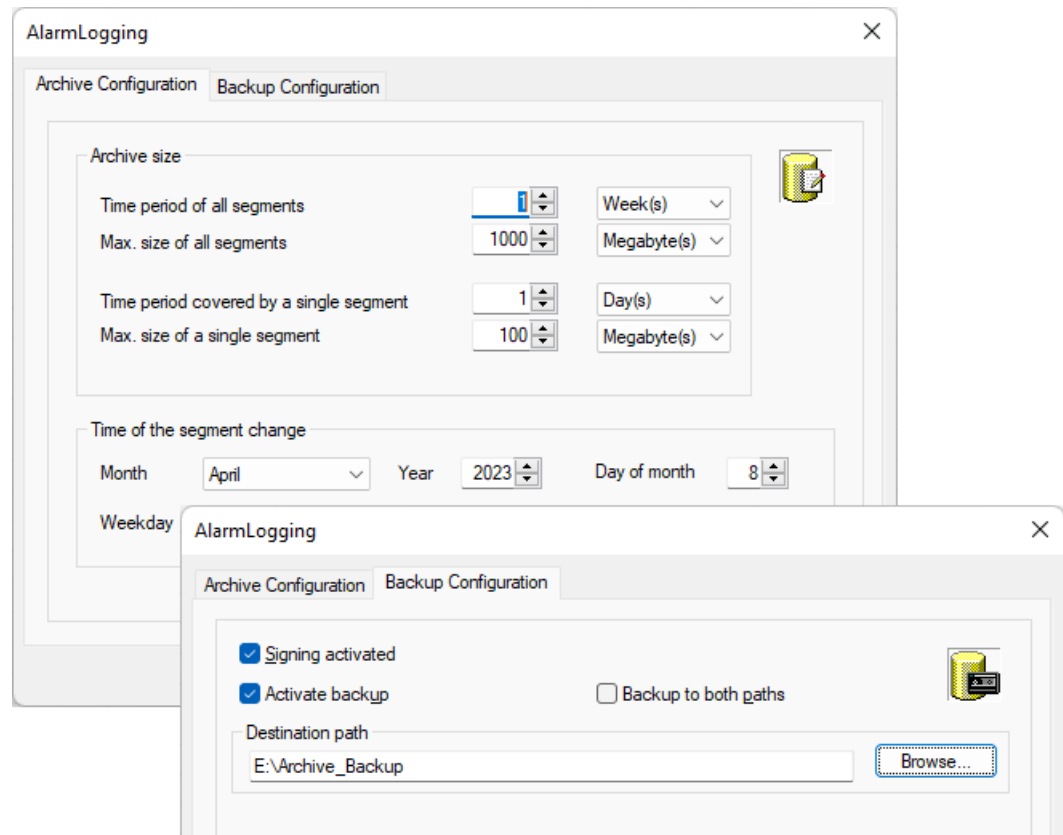


Figure 3-2 Configuration of the archiving strategy

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 standard interfaces of SIMATIC WinCC. These are also available to 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)

3.4 Audit Trail, Change Control Support

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/records during operation

SIMATIC WinCC supports the requirement of an audit trail for GMP-relevant operator actions through corresponding recording of these actions (who, what, when and, optionally, why). Such electronic records are secured through system-side security mechanisms.

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

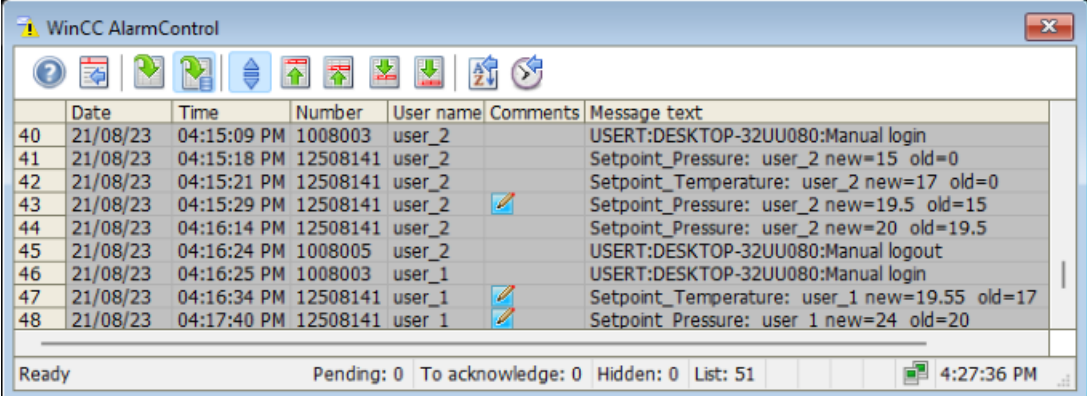
Recording process data

Process data (e.g. process values, process or operating messages) are stored without any way for the operator to change this data. No audit trail is required for this data.

Operator inputs during runtime

All changes and inputs of relevant data entered by the operator during operation are recorded in an audit trail.

Apart from alarms and system messages the operator input is also documented in the alarm log of SIMATIC WinCC.



	Date	Time	Number	User name	Comments	Message text
40	21/08/23	04:15:09 PM	1008003	user_2		USERT:DESKTOP-32UU080:Manual login
41	21/08/23	04:15:18 PM	12508141	user_2		Setpoint_Pressure: user_2 new=15 old=0
42	21/08/23	04:15:21 PM	12508141	user_2		Setpoint_Temperature: user_2 new=17 old=0
43	21/08/23	04:15:29 PM	12508141	user_2		Setpoint_Pressure: user_2 new=19.5 old=15
44	21/08/23	04:16:14 PM	12508141	user_2		Setpoint_Pressure: user_2 new=20 old=19.5
45	21/08/23	04:16:24 PM	1008005	user_2		USERT:DESKTOP-32UU080:Manual logout
46	21/08/23	04:16:25 PM	1008003	user_1		USERT:DESKTOP-32UU080:Manual login
47	21/08/23	04:16:34 PM	12508141	user_1		Setpoint_Temperature: user_1 new=19.55 old=17
48	21/08/23	04:17:40 PM	12508141	user_1		Setpoint Pressure: user_1 new=24 old=20

Ready Pending: 0 To acknowledge: 0 Hidden: 0 List: 51 4:27:36 PM

Figure 3-3 Display of the operation messages in WinCC AlarmControl

With the option WinCC/Audit the GMP-relevant variables can be defined in the configuration so that their value changes by the operator are recorded in a separate audit trail database.

More information on the option WinCC/Audit is contained in the "System Manual WinCC/Audit", see Online Support entry ID 109818158.

Configuration control

In contrast to the audit trail, changes to the system configuration are subject to the change control procedure. Such changes are planned before their execution, their potential impact evaluated, documented during execution and then tested for correct implementation. The documentation of the performed change can be supported through different tools.

Changes made to the WinCC configuration

Changes in the engineering can also be monitored with the option WinCC/Audit. This is described in more detail in the "WinCC/Audit System Manual".

Further system functions support the control of the system configuration. This includes, for example, the versioning of software elements and projects as well as functions for data backup/restore to support the corresponding procedures. For more details, see "GMP Engineering Manual SIMATIC WinCC" from Siemens.

Changes made in user management

Changes made in the course of user management (such as setup of new users, locking users, etc.) are recorded in the event log of Windows. The event log must be configured accordingly, as described in the Microsoft documentation.

For the display of the log entries from the Windows event viewer, see chapter 3.7.10 in the "WinCC/Audit System Manual".

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 an essential prerequisite for the secure operation of a system. This applies in particular for "open paths" which must be secured through additional measures. Basic principles of the security concept as well as configuration recommendations are specified in the "Security concept PCS 7 and WinCC" manual, Online Support under entry ID 109780811, as well as "Working with WinCC" in chapter 14.12, Online Support under entry ID 109818253.

SIMATIC Logon, a basic function of WinCC, is used to set up user management based on Windows security mechanisms:

- Individual users and their assignment to Windows user groups are defined in the user account control of Windows.
- SIMATIC Logon provides the link between the Windows user groups and the WinCC user groups.
- Based on user groups, user rights with different levels are defined in the user administration of SIMATIC WinCC.

The following access security requirements are thereby fulfilled:

- Central user management (setup, deactivation, blocking, unblocking, assignment to user groups) by the administrator
- Usage of a unique user ID
- Definition of access authorizations for user groups/roles
- Access and authorization levels depending on specific plant areas
- Password settings and password aging
- Prompt the user to define a new password at initial logon (initial password).
- Blocking of a user after a configurable number of failed login attempts
- Automatic logoff (auto logout) after a configurable idle time of the keyboard and mouse.
- Log functions for actions with regard to access protection

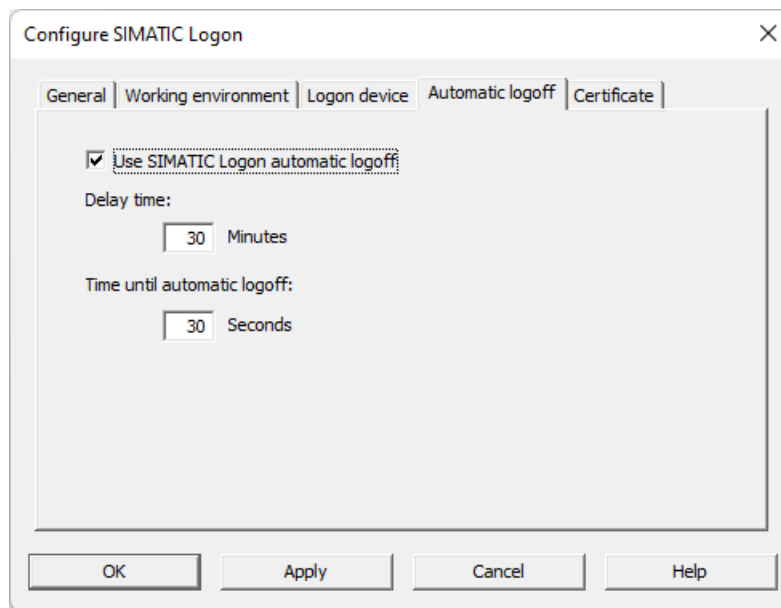


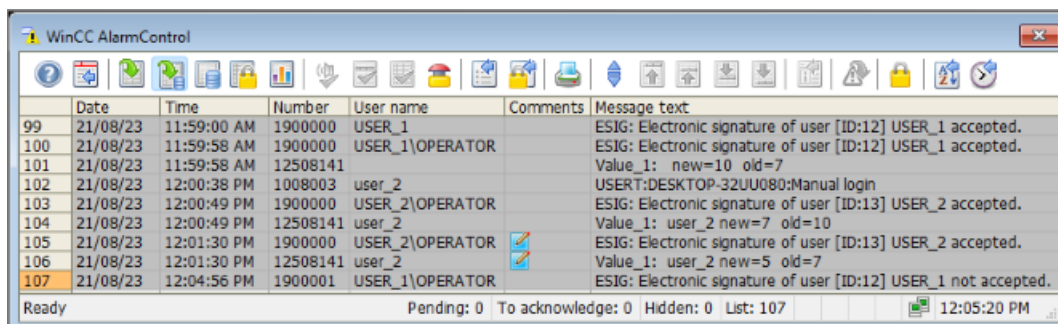
Figure 3-4 SIMATIC Logon configuration

In addition, specific access rights must be assigned to or revoked from users at operating system level to prevent unauthorized access to the directory structure of the various system programs and unintended manipulation.

3.6 Electronic Signature

SIMATIC WinCC provides functions for configuring an electronic signature. The electronic signature is rendered in the course of a dialog, if required with a mandatory comment. This applies both for the operation of WinCC objects in a process picture as well as for the acknowledging of alarms in WinCC AlarmControl.

The possibilities for configuration of an electronic signature are described in chapter 14.10 of the "Working with WinCC" System Manual, see Online Support under entry ID 109818253. Additional functions are available with the option WinCC/Audit.



	Date	Time	Number	User name	Comments	Message text
99	21/08/23	11:59:00 AM	1900000	USER_1		ESIG: Electronic signature of user [ID:12] USER_1 accepted.
100	21/08/23	11:59:58 AM	1900000	USER_1\OPERATOR		ESIG: Electronic signature of user [ID:12] USER_1 accepted.
101	21/08/23	11:59:58 AM	12508141			Value_1: new=10 old=7
102	21/08/23	12:00:38 PM	1008003	user_2		USERT:DESKTOP-32UU080:Manual login
103	21/08/23	12:00:49 PM	1900000	USER_2\OPERATOR		ESIG: Electronic signature of user [ID:13] USER_2 accepted.
104	21/08/23	12:00:49 PM	12508141	user_2		Value_1: user_2 new=7 old=10
105	21/08/23	12:01:30 PM	1900000	USER_2\OPERATOR		ESIG: Electronic signature of user [ID:13] USER_2 accepted.
106	21/08/23	12:01:30 PM	12508141	user_2		Value_1: user_2 new=5 old=7
107	21/08/23	12:04:56 PM	1900001	USER_1\OPERATOR		ESIG: Electronic signature of user [ID:12] USER_1 not accepted.

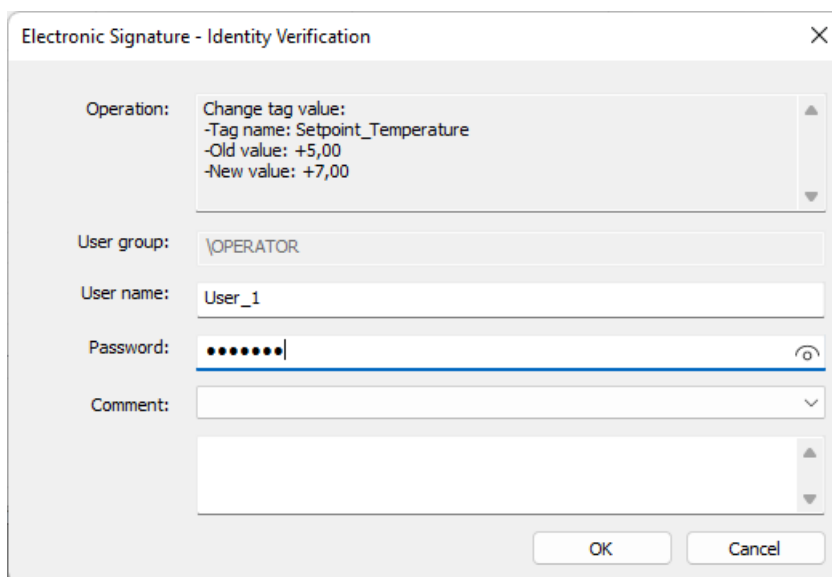
Ready Pending: 0 To acknowledge: 0 Hidden: 0 List: 107 12:05:20 PM

Figure 3-5 Representation of a message for electronic signature

Entry of an electronic signature

When performing an electronic signature, an identity check takes place for which the authorized user must authenticate themselves. The signature is recorded in the audit trail. Failed or aborted processes are also logged.

The figure shows the call for confirming an operator action with an electronic signature. The entry of a comment can be configured to be mandatory.



Electronic Signature - Identity Verification

Operation: Change tag value:
-Tag name: Setpoint_Temperature
-Old value: +5,00
-New value: +7,00

User group: \OPERATOR

User name: User_1

Password: ••••••••

Comment:

OK Cancel

Figure 3-6 Entry of an electronic signature

A multiple signature is also possible by means of the option WinCC/Audit. This means that an action has to be signed by several persons having different roles.

[illegible]

Figure 3-7 Configuration of a multiple electronic signature

More information on a multiple electronic signature is provided in the "System Manual for WinCC/Audit".

Evaluation List for SIMATIC WinCC

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 process (Product Lifecycle Management) is the development process for Siemens software products. This process incorporates risk management accordingly. During the system validation and system operation, risk management must 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 relevant steps of the lifecycle.	Annex 11, 4.1	Yes. The PLM process includes 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 in the project. The validation process is the responsibility of the regulated user.

4.1 Lifecycle and Validation of Computerized Systems

	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 should describe required functions, be risk-based and be traceable throughout the lifecycle.	Annex 11, 4.4	Yes. The specification of requirements is part of the PLM process. For the project-specific configuration the regulated user must appropriately describe the user requirements in the system's lifecycle (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 as well as test planning. The regulated user should be involved to agree upon 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 product the product's documentation is treated as being part of the product. Thus the documentation itself is subject to the requirements of the PLM process. The regulated user should establish appropriate procedural controls during development and operation of the production 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 do 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 his business continuity planning (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 to establish 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 check 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.

4.4 Audit Trail, Change Control Support

	Requirement	Reference	Answer
4.3.1	The system should provide the ability to discern invalid or altered records.	21 CFR 11.10 (a)	This can be realized with the following functions: time stamping, revisions, versioning for configuration and documents, and audit trail for operator entries.
4.3.2	For records supporting batch release, it should be possible to generate printouts indicating whether any of the data has changed since the original entry.	Annex 11, 8.2	Changes to the data through the operator are recorded in the operating log and can be printed with internal or add-on functions in the form of a report.
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 the 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 value ranges, data type check, 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, a multiple signature or operator dialog can be implemented 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 like 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 and O13).
4.3.7	Regular backups of all relevant data should be done.	Annex 11, 7.2	The regulated user should establish appropriate processes for 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	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. For example, allowances can be made for a specific sequence of operator actions by configuring the application accordingly.

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.

4.5 System Access, Identification Codes and Passwords

	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 via an audit trail and contain information with time stamp, user ID, old and new value, as well as an optional comment. 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. The operator interventions are recorded with user identification 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 should be available for review and copying by regulatory agencies.	21 CFR 11.10 (e)	Yes. The audit trail can be made available and also be exported in electronic formats.

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. The system access can be regulated via the user account control. The individual authorizations 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. Nonetheless, since system security strongly depends on the operating environment of each IT system, these aspects should be considered in security management (see GAMP 5, appendix O11). Recommendations and support is given by Siemens' Industrial Security approach.
4.5.3	Creation, change, and cancellation of access authorizations should be recorded.	Annex 11, 12.3	Changes in user access management are recorded and should be subject to change control procedures of the regulated user.

4.5 System Access, Identification Codes and Passwords

	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. WinCC workstations can be configured so that special input data/commands can only be performed from a dedicated workstation, or from a group of dedicated workstations. In this case, all other workstations have read-only access rights at the most. The system performs verifications, because the stations must be interconnected within the system.
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 each user identification is unique within the system. Thus each combination of user identification and password are unique.
4.5.6	Procedures are in place to ensure that the validity of identification codes is checked periodically.	21 CFR 11.300 (b) Annex 11, 11	The regulated user should establish appropriate procedural controls.
4.5.7	Passwords should periodically expire and have to be revised.	21 CFR 11.300 (b)	Yes. Password aging can be configured in the user management.
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 deactivated or the assigned permission can be withdrawn from the user. The regulated user should 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 should establish appropriate procedural controls.

	Requirement	Reference	Answer
4.5.10	Measures for detecting attempts of unauthorized use and for informing security and management should be in place.	21 CFR 11.300 (d) Annex 11, 12.1	Yes. Failed 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 Siemens range of products, but can be integrated into the system by means of SIMATIC Logon. The regulated user should 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. The listed information is available.
4.6.3	The above-listed information is shown on displayed and printed copies of the electronic record.	21 CFR 11.50 (b)	Yes. The listed information is available.
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. The electronic signatures cannot be removed or used otherwise.

4.7 Open Systems

	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 in the user administration of the Windows operating system. 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 about 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 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. Support is provided, for example, based on the configuration information in the "Security Concept PCS 7 and WinCC" manual, as well as by commonly available standard tools for encryption. SSL encryption for the data communication of the terminal bus is one of these possible measures. Certificates for an encrypted WinCC connection can be created with the certificate management.
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 does not provide functionality for digital (encrypted) signatures.

4.7 Open Systems

Get more information

Siemens AG
Digital Industries
Pharmaceutical and Life Science Industry
Siemensallee 84
76187 Karlsruhe, Germany
PDF (A5E52749113-AA)
Produced in Germany

Subject to changes and errors. The information given in this catalog only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products.

The requested performance features are binding only when they are expressly agreed upon in the concluded contract. All product designations may be trademarks or product names of Siemens AG or other companies whose use by third parties for their own purposes could violate the rights of the owners.