

Compliance Response Edition 07/2009



SIMATIC WinCC V7.0
Compliance Response
Electronic Records / Electronic Signatures

simatic winCC

DOKUMENTATION

SIEMENS

**Compliance Response
Electronic Records / Electronic Signatures
for SIMATIC WinCC V7.0**

SIEMENS AG

Industry Sector

I IA VMM Pharma

D-76187 Karlsruhe, Germany

E-mail: pharma.aud@siemens.com

July 2009

Table of Contents

Table of Contents	2
Introduction.....	3
1 The Requirements in Short.....	4
2 Meeting the Requirements with SIMATIC WinCC.....	5
2.1 Technological solution for access security.....	5
2.2 Technological solution for audit trail.....	6
2.3 Technological solution for data archiving and retrieval.....	8
2.4 Technological solution for electronic signatures	8
3 Evaluation List for SIMATIC WinCC.....	9
3.1 Procedures and controls for closed systems	9
3.2 Additional procedures and controls for open systems	11
3.3 Signed electronic records.....	12
3.4 Electronic signatures (general)	13
3.4.1 Electronic signatures (non-biometric)	13
3.4.2 Electronic signatures (biometric).....	14
3.5 Controls for identification codes and passwords	14

Introduction

In August 1997, the regulation 21 CFR Part 11 “Electronic Records; Electronic Signatures” of the US regulatory agency Food and Drug Administration (FDA) was enacted. 21 CFR Part 11 (in short: Part 11) defines the FDA acceptance criteria for the use of electronic records and electronic signatures in place of records in paper form and handwritten signatures on paper. In this regard, electronic records and signatures must be as trustworthy, reliable and effective as conventional records. The FDA regulations are also applied beyond the pharmaceutical industry in other life sciences, such as the food and beverage industry, cosmetics, consumer care, etc.

In 1992, the European Commission had already defined requirements for the use of computerized systems in Annex 11 to the EU GMP Guideline¹ (in short: Annex 11). However, by contrast to Part 11 of FDA, although this guideline covers all topics related to computerized systems, it lacks the in-depth details with regard to electronic records and electronic signatures as provided in 21 CFR Part 11.

Application of regulations such as Part 11 and the EU GMP Guideline (or its corresponding implementation in national legislation) is mandatory for the use of electronic records and electronic signatures. However, these regulations are only valid within their relevant national context, applying only to “regulated” electronic records. Beyond the use of electronic records and signatures, conventional paper documents and handwritten signatures, or a combination of both, can still be used.

The statutory code relating to this subject matter is supplemented by diverse interpretation methods and recommendations of regulatory authorities such as the FDA and industry associations such as ISPE and PDA. This document is based on the current interpretation of the ISPE CoP GAMP² and PDA³ that is accepted worldwide. If the interpretation of a requirement by a company differs from the requirement specified here, please contact the IIA VMM Pharma department of Siemens AG in Karlsruhe for more information (see contact information above).

To help our clients, Siemens as supplier of SIMATIC WinCC evaluated version 7.0 of the system with regard to these requirements. Due to its closer itemization, this analysis is based on the detailed requirements specified in Part 11 (FDA), however, while making implicit allowances for requirements to Annex 11 (EU). The results of this assessment are published in this document.

SIMATIC WinCC V7.0 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 client.

The Siemens recommendations for the system architecture, conception, and configuration will assist system users in achieving compliance. For additional information and assistance see “GMP Engineering Manual SIMATIC WinCC”⁴.

This document is divided into three parts: The first part provides a brief overview of the requirements of Part 11, the second introduces the functionality of SIMATIC WinCC V7.0 under the aspect of those requirements, and the third contains a detailed system assessment on the basis of the single requirements of Part 11.

¹ EU Guidelines to Good Manufacturing Practice, Volume 4, Medicinal Products for Human and Veterinary Use, Annex 11 Computerized Systems; European Commission Brussels, 2005

² GAMP Good Practice Guide “A Risk-Based Approach to Compliant Electronic Records and Signatures”; ISPE 2005

³ Good Practice and Compliance for Electronic Records and Signatures, Part 2 “Compliance with 21 CFR Part 11, Electronic Records and Electronic Signatures”; ISPE and PDA 2001/2002

⁴ GMP Engineering Manual, SIMATIC WinCC; Siemens AG, I IA VMM Pharma

1 The Requirements in Short

21 CFR Part 11 takes into account that the risk of manipulation, misinterpretation and changes without trace is higher with electronic records and electronic signatures than with conventional paper records and handwritten signatures, or are more difficult to detect. Additional measures are required for this reason.

The terms "electronic record" / "electronic document" mean 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.⁵

The term "electronic signature" means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.⁵

Requirement	Description
Validation	All GMP-relevant automated systems must be validated to ensure precise, reliable and consistent data preparation in accordance with the standards.
Audit Trails	All regulated operator actions which create, modify or delete electronic records must be recorded in a secure, time-stamped, computer-generated audit trail.
Record retention, Protection, Reproducibility and Retrievability	Systems must have the capability to retain, protect and readily retrieve records throughout the established retention period. Systems must be able to reproduce electronic records in both human readable and electronic form.
Document Controls	Controls must exist over access, revision, distribution, and use of documentation for system operation and maintenance.
Access Control	Systems must limit access to only authorized, qualified personnel. In open systems, additional security measures must be implemented to ensure this (see also 21 CFR 11.30).
Electronic Signature	Systems must provide measures to ensure that utilization is limited to the genuine owner only and that attempted use by others is promptly detected and recorded. Non-biometric systems must provide two distinct identification components (e.g. user ID and password) to be entered when signing. At least the password must be re-entered for any subsequent signing action within the same session. Electronic signatures must not be reused or reassigned. The purpose of an electronic signature must be clearly indicated. Finally, systems must include measures to prohibit falsification of electronic signatures using standard tools. Written policies must be in place, which hold individuals responsible for actions initiated under their electronic signatures.
Certificate to FDA	Written certification must be provided to the FDA Office of Regional Operations that all electronic signatures in use are the legally binding equivalent of traditional handwritten signatures.

⁵Good Practice and Compliance for Electronic Records and Signatures; Part 2 "Complying with 21 CFR Part 11, Electronic Records and Electronic Signatures"; ISPE and PDA 2001/2002

2 Meeting the Requirements with SIMATIC WinCC

The requirements, which can be fulfilled by technological solutions, can be summarized under four topics:

- Access security
- Audit trail
- Data archiving and retrieval
- Electronic signature

2.1 Technological solution for access security

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

- Individual users and their assignment to Windows user groups are defined in the Windows user administration.
- 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.

Thereby the following access security requirements are fulfilled:

- Central user management (setup, deactivation, blocking, unblocking, assignment to user groups) by the administrator
- Unique combination of a user identification (user ID) and password
- Definition of access rights for groups and users
- Access and authorization levels depending on specific plant areas
- Password aging: The user is forced to change his/her password on expiration of a configurable time; the password can be reused only after "n" generations.
- The system can prompt the user to define a new password at initial logon (initial password).
- The user is automatically blocked after a configurable number of failed logon attempts and can only be unblocked by the administrator.
- Automatic logoff (auto-logout) after a configurable idle time of the keyboard and mouse
- Log functions for actions related to access security, such as logon, manual and automatic logoff, input of incorrect user ID or password, user blocked after several attempts to enter an incorrect password, and password change by user.

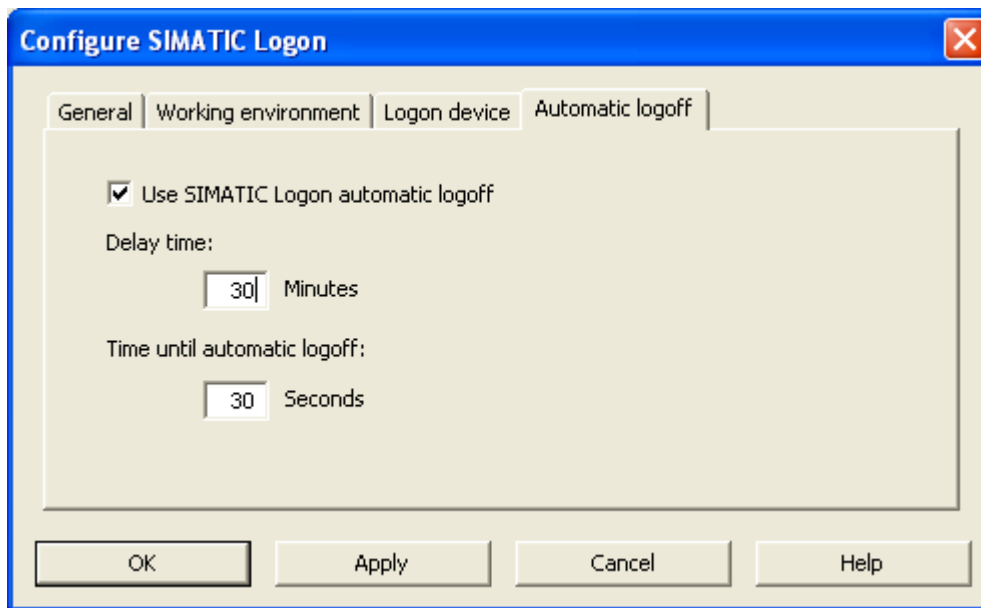


Figure 1: SIMATIC Logon configuration

SIMATIC Logon meets the requirements regarding access security in combination with procedural controls, such as those for "specifying the responsibility and access permission of the system users".

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

If system access is not controlled by persons who are responsible for the content of the electronic records, the system is defined as "open". Additional security mechanisms need to be set up for any "open paths" which might exist. For more information on the basic policies of the security concept and configuration recommendations, refer to the "Security Concept PCS 7 and WinCC" manual.

2.2 Technological solution for audit trail

Audit trails are of particular importance in areas where operator actions generate, modify, or delete data in the course of normal operation. An audit trail is not required for automatically generated electronic records which can neither be modified, nor be deleted by the operator. SIMATIC WinCC provides adequate system security for such electronic records (e.g. access control).

The following section describes how the SIMATIC WinCC system supports the implementation of requirements with regard to the audit trails during runtime operation. Moreover, it also informs about the system support for tracing changes made in the engineering system.

Runtime phase

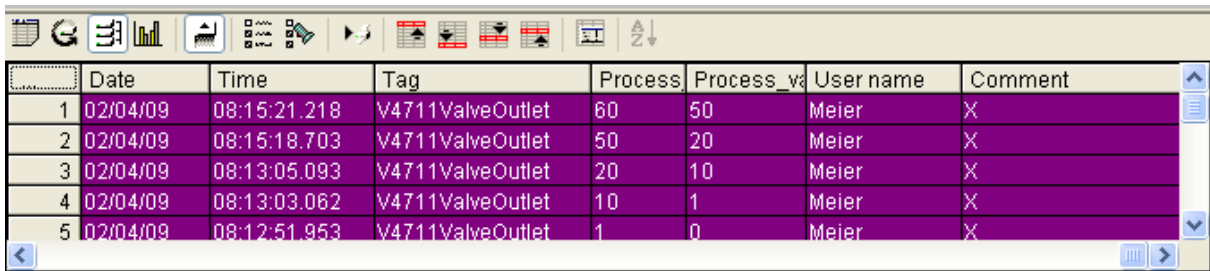
Logging of process data

Process data (e.g. process values, process or operating messages) are stored without any option for the operator to change this data.

Changes during runtime

All runtime changes and entries made by the operator in the process visualization system must be logged to an audit trail. SIMATIC WinCC provides various options to this effect.

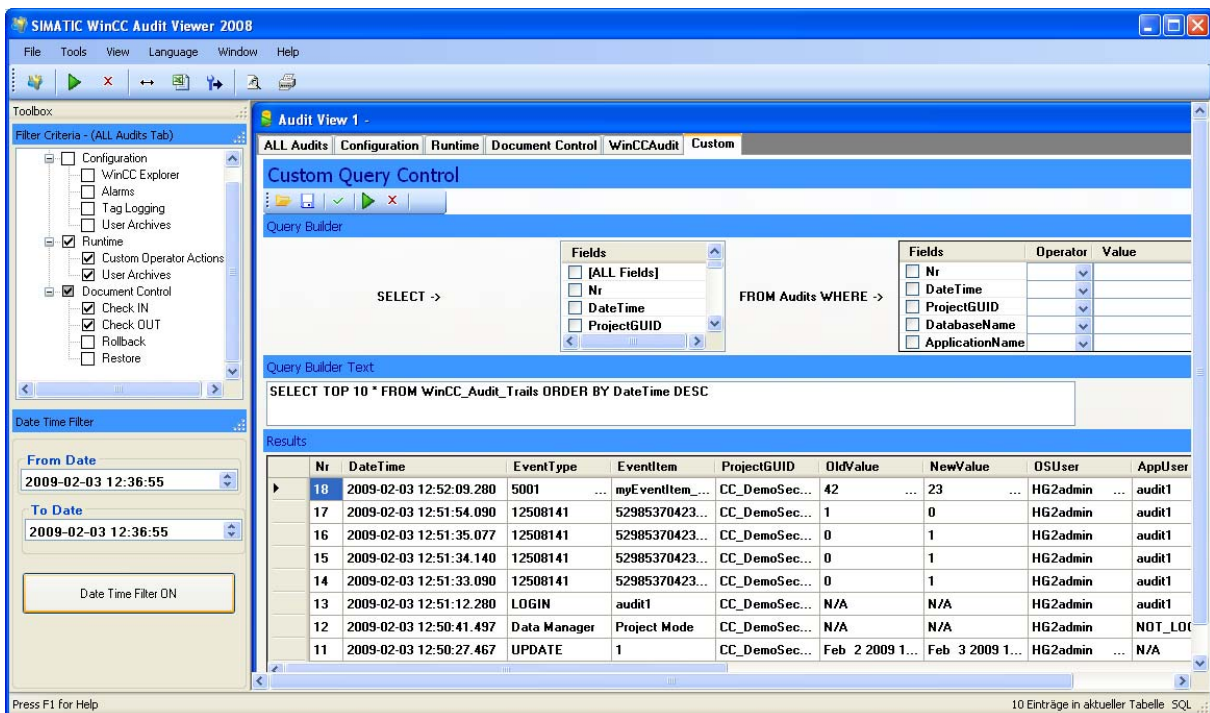
Logging and visualization of operator input actions by means of WinCC message archive:



	Date	Time	Tag	Process	Process_v	User name	Comment
1	02/04/09	08:15:21.218	V4711ValveOutlet	60	50	Meier	X
2	02/04/09	08:15:18.703	V4711ValveOutlet	50	20	Meier	X
3	02/04/09	08:13:05.093	V4711ValveOutlet	20	10	Meier	X
4	02/04/09	08:13:03.062	V4711ValveOutlet	10	1	Meier	X
5	02/04/09	08:12:51.953	V4711ValveOutlet	1	0	Meier	X

Figure 2: Display of the audit trail by means of Alarm Logging

Logging and visualization of operator input actions by means of the "WinCC/Audit" option:



Custom Query Control

Query Builder

SELECT -> FROM Audits WHERE ->

Query Builder Text

```
SELECT TOP 10 * FROM WinCC_Audit_Trails ORDER BY DateTime DESC
```

Results

Nr	DateTime	EventType	EventItem	ProjectGUID	OldValue	NewValue	OSUser	AppUser
18	2009-02-03 12:52:09.280	5001	myEventItem...	CC_DemoSec...	42	23	HG2admin	audit1
17	2009-02-03 12:51:54.090	12508141	52985370423...	CC_DemoSec...	1	0	HG2admin	audit1
16	2009-02-03 12:51:35.077	12508141	52985370423...	CC_DemoSec...	0	1	HG2admin	audit1
15	2009-02-03 12:51:34.140	12508141	52985370423...	CC_DemoSec...	0	1	HG2admin	audit1
14	2009-02-03 12:51:33.090	12508141	52985370423...	CC_DemoSec...	0	1	HG2admin	audit1
13	2009-02-03 12:51:12.280	LOGIN	audit1	CC_DemoSec...	N/A	N/A	HG2admin	audit1
12	2009-02-03 12:50:41.497	Data Manager	Project Mode	CC_DemoSec...	N/A	N/A	HG2admin	NOT_LOC
11	2009-02-03 12:50:27.467	UPDATE	1	CC_DemoSec...	Feb 2 2009 1...	Feb 3 2009 1...	HG2admin	N/A

Figure 3: Display of the audit trail by means of WinCC/Audit

Configuration phase

Changes made during configuration

To provide support of a formal Change Control method, the WinCC/ChangeControl option can log changes made to the WinCC projects (e.g. archives, graphic objects, setup of user rights, etc.). WinCC/ChangeControl is available either as a separate option, or as a component of WinCC/Audit. The Document Control function of WinCC/Audit integrated in WinCC/ChangeControl provides a comprehensive means of monitoring the check in, check out, deletion, reset (rollback) and restoration of application and user documents. Copies of all configuration states of a document are saved to a secure database.

Changes made in user management

Changes made in the course of user management (e.g. setup of new users, blocking users, etc.) are recorded in the event log of Windows. The event log must be configured accordingly.

2.3 Technological solution for data archiving and retrieval

Continuous archiving

SIMATIC WinCC provides a configurable and scalable archiving concept. Messages and measured values are stored continuously to local WinCC archives. These locally stored data can be transferred automatically to long-term archives. Generation of checksums prevents any unauthorized manipulation of the archived data. Archive data can be retrieved within the entire, configured retention period. Data can be retrieved within SIMATIC WinCC using either standard functions, or additional standard interfaces, or optional packages (e.g. DataMonitor, Connectivity Pack).

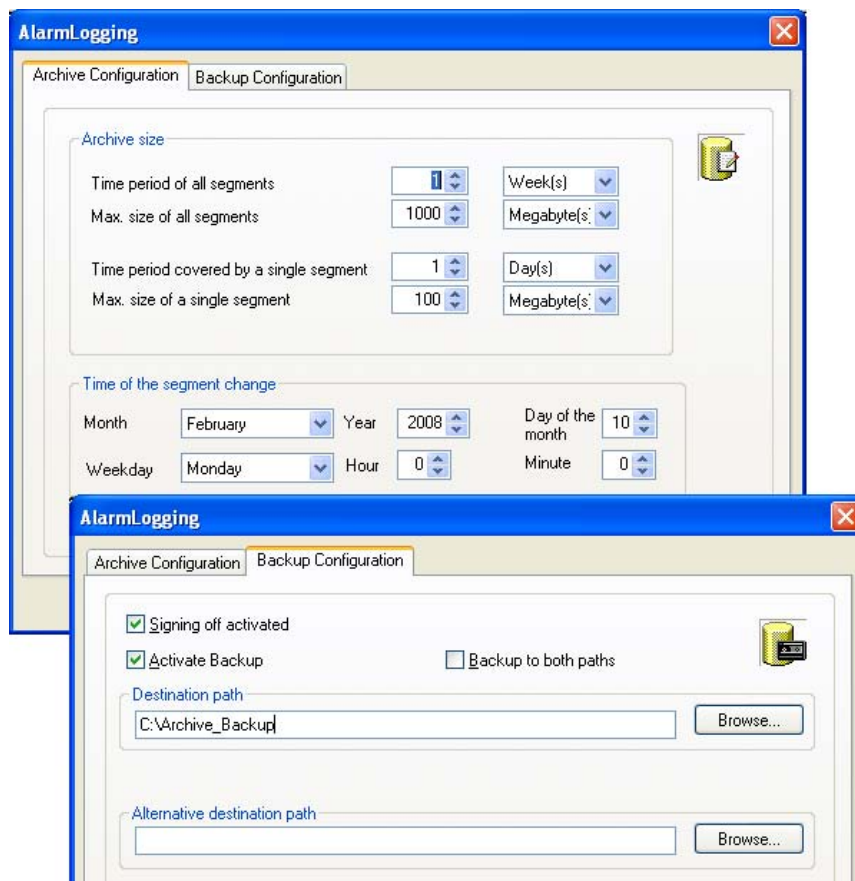


Figure 4: Archive configuration

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).

2.4 Technological solution for electronic signatures

SIMATIC WinCC provides functions for configuring an electronic signature. The electronic signature is executed in a dialog. The user ID and password are requested and verified for the purpose of identification.

3 Evaluation List for SIMATIC WinCC

The following checklist for a system assessment originates from a document of ISPE / PDA⁶.

The system assessment checklist covers all requirements, not only those which can be satisfied by technological solutions. To meet certain requirements of 21 CFR Part 11, the pharmaceutical company must implement corresponding procedural controls. The rules and standards always relate to the customer-specific application that was implemented with SIMATIC WinCC. Therefore, the solutions then specified are valid only in conjunction with specific procedures and organizational measures.

3.1 Procedures and controls for closed systems

If system access is controlled by persons who are responsible for the content of the electronic records, then the system is defined as "closed" and must be assessed against the requirements of this section.

Paragraph/ detail	Questions / requirements	Comments
11.10(a) detail 1	Is the system validated?	<p>The customer is responsible for the validation of the application or system. The validation should follow an established system life cycle (SLC) methodology, e.g. as described in the GAMP guidelines.</p> <p>SIMATIC WinCC has been developed in compliance with the Siemens Quality Management System (certified to ISO 9001:2008).</p> <p>Siemens supports validation of the application during projects upon request.</p>
11.10(a) detail 2	Is it possible to discern invalid or altered records?	<p>Yes.</p> <p>An entry can be generated in the audit trail for any operator action (such as modification of setpoints / alarm limits / monitoring modes, or alarm acknowledgments). All relevant changes are logged, including the time stamp, user ID, old and new value, and comments. Unauthorized changes are prevented by the access security function of the system.</p> <p>Archived records are protected with a checksum mechanism to detect any unauthorized changes.</p> <p>Changes within the configuration of SIMATIC WinCC can be traced using WinCC/Audit.</p>
11.10(b) detail 1	Is the system capable of producing accurate and complete copies of electronic records on paper?	<p>Yes.</p> <p>SIMATIC WinCC provides printed copies of process values, messages and audit trails.</p>

⁶ Good Practice and Compliance for Electronic Records and Signatures; Part 2 "Compliance with 21 CFR Part 11, Electronic Records and Electronic Signatures"; ISPE and PDA 2001/2002

Paragraph/ detail	Questions / requirements	Comments
11.10(b) detail 2	Is the system capable of producing accurate and complete copies of records in electronic form for inspection, review and copying by the FDA?	Yes. Process values, messages and audit trails can be exported in electronic format and be visualized using WinCC or the DataMonitor option. The WinCC/Audit option can be used to export the audit trail to Microsoft Excel, PDF, CSV or XML file format.
11.10(c)	Are the records readily retrievable throughout their retention period?	Yes. Records can be archived in a readable format, e.g. on CD or DVD. We assume that these devices and formats will also be readable in the future. Records swapped to the archive can be viewed using the DataMonitor option or be retrieved to WinCC. Clients should specify retention periods and define procedures for archiving, backup and retrieval of electronic records.
11.10(d)	Is system access limited to authorized individuals?	Yes. All options of the Windows user management are active when SIMATIC Logon is being used (refer to chapter 2.1 Technological solution for access security). Customers should ensure that only persons who have a legitimate reason to use the system should be granted access to the system (e.g. server, system console). As this requirement is virtually equivalent to 11.10(g), it is generally interpreted to refer to both physical access and logical access.
11.10(e) detail 1	Is there a secure, computer generated, time stamped audit trail that records the date and time of operator entries and actions that create, modify, or delete electronic records?	Yes. The audit trail is secure within the system and cannot be changed by a user. Changes during production can be traced back by the system itself and contain information with time stamp, user ID, old and new value and comment.
11.10(e) detail 2	Upon making a change to an electronic record, is previously recorded information still available (i.e., not obscured by the change)?	Yes. Recorded information is not overwritten and is always available in the database.
11.10(e) detail 3	Is an electronic record's audit trail retrievable throughout the record's retention period?	Yes. The audit trail can be made available during the entire retention period. (see 11.10 (c))
11.10(e) detail 4	Is the audit trail available for review and copying by the FDA?	Yes. The WinCC/Audit option can be used to export the audit trails to Microsoft Excel, PDF, CSV or XML file format. An audit trail recorded in Alarm Logging can be exported in PDF or CSV format.
11.10(f)	If the sequence of system steps or events is important, is this enforced by the system (e.g., as would be the case in a process control system)?	Yes. Allowances can be made for a specific sequence of operator actions by configuring the application accordingly.

Paragraph/ detail	Questions / requirements	Comments
11.10(g)	Does the system ensure that only authorized individuals can use the system, electronically sign records, access the operation or computer system input or output device, alter a record, or perform other operations?	Yes. The SIMATIC Logon software package is based on the security system of MS Windows. The user ID and password are being used. Central user management is used in this regard for managing users and user groups. In addition, the customer should define how access is limited to authorized individuals (e.g. who has access to specific objects or functions within WinCC Runtime?), including the special rights for administrators.
11.10(h)	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.)	Yes. The 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. All other workstations then have only read-access rights at the most. The system performs verifications because the stations must be interconnected within the system.
11.10(i)	Is there documented training, including on-the-job training for system users, developers, IT support staff?	Yes. Siemens offers either standard training courses, or training related to customer projects which must be planned and performed separately. The customer is responsible for initiating and performing the training courses.
11.10(j)	Is there a written policy that makes individuals fully accountable and responsible for actions initiated under their electronic signatures?	Customers are responsible for providing procedural controls.
11.10(k) detail 1	Is the distribution of, access to, and use of system operation and maintenance documentation controlled?	
11.10(k) detail 2	Is there a formal change control procedure for system documentation that maintains a time sequenced audit trail for those changes made by the pharmaceutical organization?	

3.2 Additional procedures and controls for open systems

If system access is **not** controlled by persons who are responsible for the content of the electronic records, then the system is defined as “open” and must in addition be assessed against the requirements of this section. SIMATIC WinCC can be operated in both a closed and an open environment. Additional requirements must be met in the implementation for open systems.

Paragraph/ detail	Questions / requirements	Comments
11.30 detail 1	Is data encrypted?	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, or by commonly available standard tools for encryption.
11.30 detail 2	Are digital signatures used?	SIMATIC WinCC does not provide any functionality for digital (encrypted) signatures. Certain standard tools are available on the market which support digital signatures for records (e.g. for PDF files).

3.3 Signed electronic records

Paragraph/ detail	Questions / requirements	Comments
11.50 detail 1	Do signed electronic records contain the following related information? a) Printed name of the signer b) Date and time of signing c) Meaning of the signing (such as approval, review, responsibility)	Yes. Signed electronic records include the following information: a) Printed name or user ID of the signer b) Date and time of signing c) Including the meaning
11.50 detail 2	Is the above information shown on displayed and printed copies of the electronic record?	Yes. The information mentioned above can be displayed and printed as a component of the electronic record.
11.70	Are signatures linked to their respective electronic records to ensure that they cannot be cut, copied, or otherwise transferred by ordinary means for the purpose of falsification?	Yes. As soon as an electronic record is signed, it is stored to the WinCC database. This record cannot be copied, modified, or deleted. External access to the database is protected by password. It is also advisable to implement the Windows security functions to restrict access to the database.

3.4 Electronic signatures (general)

Paragraph/ detail	Questions / requirements	Comments
11.100(a) detail 1	Are electronic signatures unique to an individual?	Yes. The electronic signature uses the user ID and password of the user. The uniqueness of the user ID is ensured by the MS Windows security system. It is not possible to define more than one user with the same user ID within a workgroup / domain. In addition, the customer must ensure the uniqueness of the electronic signature to an individual.
11.100(a) detail 2	Are electronic signatures ever reused by or reassigned to anyone else?	The customer has to ensure and is responsible that a user ID is assigned to one individual only.
11.100(b)	Is the identity of an individual verified before an electronic signature is allocated?	This remains the responsibility of customers. Customers must take corresponding organizational measures.

3.4.1 Electronic signatures (non-biometric)

Paragraph/ detail	Questions / requirements	Comments
11.200 (a)(1)(i)	Is the signature made up of at least two components, such as a user ID and password, or an ID card and password?	Yes. SIMATIC Logon identifies the person with two distinct components, e. g. user ID and password.
11.200 (a)(1)(ii)	When several signings are made during a continuous session, is the password executed at each signing? (Note: both components must be executed at the first signing of a session)	Yes. Each signature requires at least two components (user ID and password).
11.200 (a)(1)(iii)	If signings are not done in a continuous session, are both components of the electronic signature executed for each signing?	Yes. Each signature requires at least two components (user ID and password).
11.200 (a)(2)	Are non-biometric electronic signatures only used by their genuine owners?	The customer is responsible for providing procedural controls that prevent the disclosure of passwords.
11.200 (a)(3)	Would an attempt to falsify an electronic signature require the collaboration of at least two individuals?	Yes. It is not possible to falsify an electronic signature during signing and after the system has written it into a record. The administrator cannot misuse the signature, although he configures the user ID and initial password, because the user is forced to change his password at the first logon. Unauthorized use of user IDs / passwords (failed logon attempts) is detected and logged immediately. In addition, the customer needs procedures that prevent the disclosure of passwords.

3.4.2 Electronic signatures (biometric)

Para-graph/detail	Questions / requirements	Comments
11.200(b)	Has it been shown that biometric electronic signatures can be used only by their genuine owner?	Standard tools of third-party manufacturers can be used to create biometric electronic signatures. The integrity of such solutions should be assessed separately.

3.5 Controls for identification codes and passwords

Paragraph/detail	Questions / requirements	Comments
11.300(a)	Are controls in place to maintain the uniqueness of each combined identification code and password, such that no individual can have the same combination of identification code and password?	See 11.100(a).
11.300(b) detail 1	Are procedures in place to ensure that the validity of identification codes is periodically checked?	The customer is responsible for providing procedural controls.
11.300(b) detail 2	Do passwords periodically expire and need to be revised?	Yes. A password expires after a specified number of days and cannot be reused for a specified number of generations according to MS Windows security parameters. Password aging has no effect on prior usage (records, signatures).
11.300(b) detail 3	Is there a procedure for recalling identification codes and passwords if a person leaves or is transferred?	The customer is responsible for creating procedural controls. The MS Windows security system can be used to deactivate user accounts.
11.300(c)	Is there a procedure for electronically disabling an identification code or password if it is potentially compromised or lost?	The customer is responsible for creating procedural controls. The MS Windows security system can be used to modify user accounts. The user can change his password at any time using SIMATIC Logon.
11.300(d) detail 1	Is there a procedure for detecting attempts at unauthorized use and for informing security?	Unauthorized logon attempts are logged to the MS Windows security log. The user account is blocked after a specified number of unauthorized attempts. In addition, the customer is responsible for providing appropriate organizational measures.
11.300(d) detail 2	Is there a procedure for reporting repeated or serious attempts at unauthorized use to management?	The customer is responsible for providing appropriate organizational measures.

For tokens, cards, and other devices bearing or generating identification code or password information

Paragraph/ detail	Questions / requirements	Comments
11.300(c) detail 1	Is there a loss management procedure to be followed if a device is lost or stolen?	Not applicable for pure software products like SIMATIC WinCC.
11.300(c) detail 2	Is there a procedure for electronically disabling a device if it is lost, stolen, or potentially compromised?	Not applicable for pure software products like SIMATIC WinCC.
11.300(c) detail 3	Are there controls over the issuance of temporary and permanent replacements?	Not applicable for pure software products like SIMATIC WinCC.
11.300(e) detail 1	Is there initial and periodic testing of tokens and cards?	Not applicable for pure software products like SIMATIC WinCC.
11.300(e) detail 2	Does this testing check that there have been no unauthorized alterations?	Not applicable for pure software products like SIMATIC WinCC.

A5E02546072-01

Siemens Aktiengesellschaft

Industry Sector

Industry Automation

VMM Pharmaceutical

76181 KARLSRUHE

GERMANY

pharma.aud@siemens.com

www.siemens.com/simatic-wincc