

Compliance Response Edition 06/2009



**SIMATIC WinCC flexible 2008**  
Compliance Response  
Electronic Records / Electronic Signatures

simatic hmi  
DOCUMENTATION

**SIEMENS**

**Compliance Response**  
**Electronic Records / Electronic Signatures**  
**for SIMATIC WinCC flexible 2008**

SIEMENS AG

Industry Sector

I IA VMM Pharma

D-76187 Karlsruhe, Germany

Email: [pharma.aud@siemens.com](mailto:pharma.aud@siemens.com)

June 2009

# Table of Contents

<b>Table of Contents .....</b>	<b>2</b>
<b>Introduction.....</b>	<b>3</b>
<b>1 The Requirements in Short.....</b>	<b>4</b>
<b>2 Meeting the Requirements with SIMATIC WinCC flexible .....</b>	<b>5</b>
2.1 Technological solution for access security .....	5
2.2 Technological solution for audit trail .....	8
2.3 Technological solution for data archiving and retrieval .....	9
2.4 Technological solution of electronic signatures.....	10
<b>3 Evaluation List for SIMATIC WinCC flexible .....</b>	<b>11</b>
3.1 Procedures and controls for closed systems.....	11
3.2 Additional procedures and controls for open systems .....	14
3.3 Signed electronic records .....	14
3.4 Electronic signatures (general).....	15
3.4.1 Electronic signatures (non biometric) .....	15
3.4.2 Electronic signature (biometric) .....	16
3.5 Controls for identification codes and passwords .....	16

# 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 Guideline<sup>1</sup> (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 GAMP<sup>2</sup> and PDA<sup>3</sup> 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 flexible evaluated version 2008 SP1 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 flexible 2008 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 flexible”<sup>4</sup>.

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 flexible 2008 under the aspect of those requirements, and the third contains a detailed system assessment on the basis of the single requirements of Part 11.

---

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

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

<sup>3</sup> 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

<sup>4</sup> GMP Engineering Manual, SIMATIC WinCC flexible; Siemens AG, IIA 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 records” / “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.<sup>5</sup>

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.<sup>5</sup>

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 certifications must be provided to the FDA Office of Regional Operations that all electronic signatures un use are the legally binding equivalent of traditional handwritten signatures.

---

<sup>5</sup> Good 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 flexible

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

Users must be only assigned the required access rights at operation system level to prevent unauthorized access to the file system and the directory structures of the system programs, to the configured data and the runtime data and unintended manipulation.

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". Additional security mechanisms need to be set up for any "open paths" which might exist.

The user management configuration is performed centrally on an engineering system for each application and uploaded from there to the respective HMI device (PC or panel).

SIMATIC WinCC flexible supports both local and central user management to ensure protection of electronic records.

#### Local user management

With local user management, individual users and their assignment to user groups are only known locally.

- Individual users and their assignment to user groups are defined in the WinCC flexible configuration.
- Based on user groups, user right with different levels are defined in the user administration of WinCC flexible.

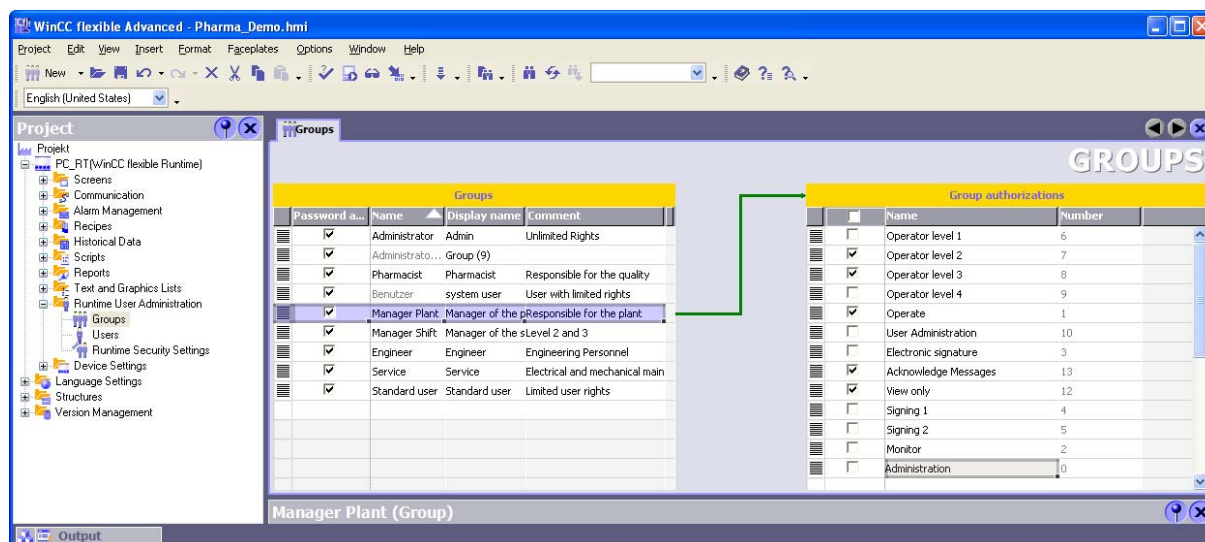


Figure 1: Assignment of user rights to user groups

Thereby the following access security requirements are fulfilled:

- Users can only log on to the HMI device with a unique combination of user ID and password.
- Users can change their own password locally on the HMI device.
- The following settings with regard to password security are possible:
  - Password with at least one special character
  - Password with at least one digit
  - Minimum password length between 3 and 24 characters
- Password aging is supported, and the validity period of a password and the number of generations can be configured.
- The system can force the user to change the initial password at the first logon.
- The user is automatically blocked after a configurable number of failed logon attempts and can be unblocked only by the administrator.
- The system automatically logs off users after a configurable time period with no activity.
- Log functions for actions related to access security in the audit train, 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.

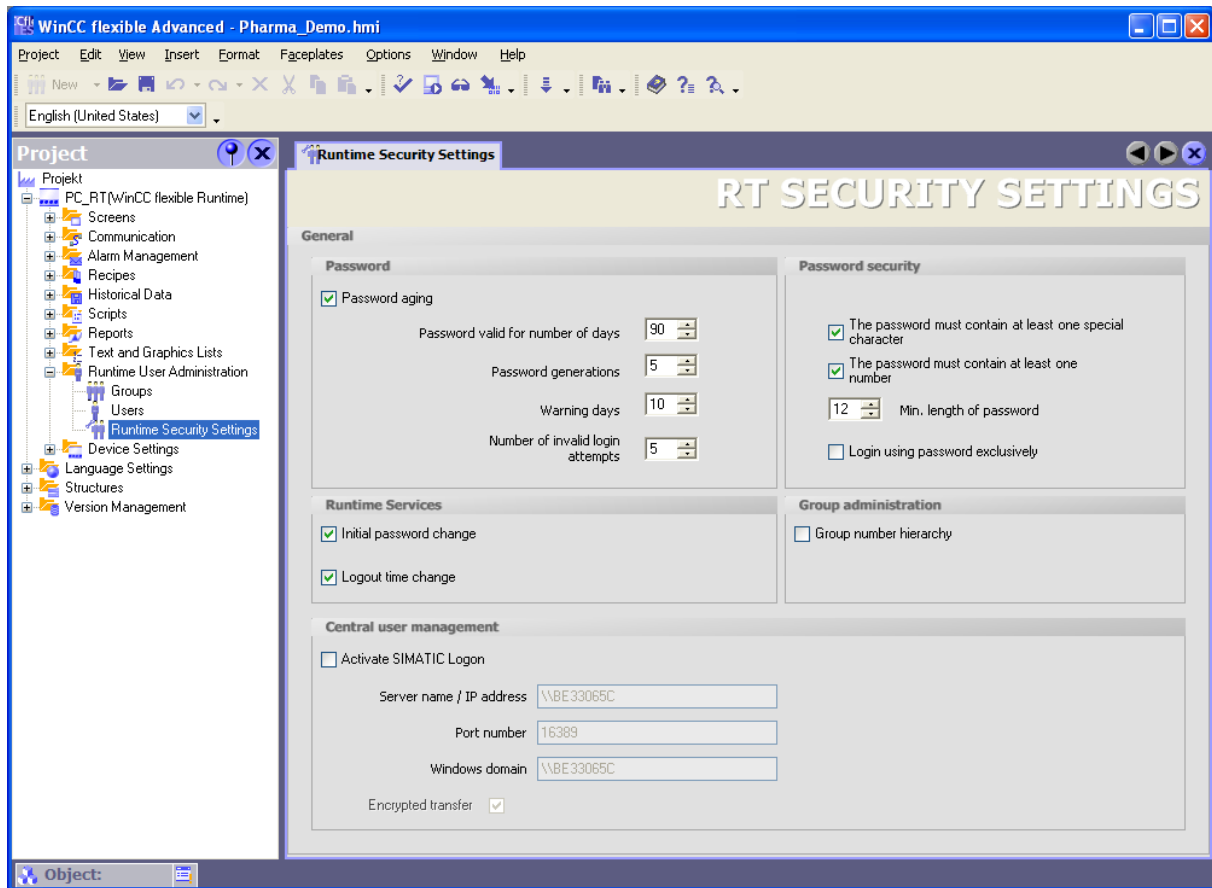


Figure 2: Configuration on the security settings of the user administration

## Central user management

The central user management is implemented with the software package SIMATIC Logon<sup>6</sup>. SIMATIC Logon is installed in a central computer with an MS Windows operating system (the supported operating systems can be found in the Release Notes of SIMATIC Logon). User management based on MS Windows security mechanisms is set up there. The HMI devices are connected to the computer via Ethernet.

- Individual users and their assignment to Windows user groups are defined in the user management of Windows.
- Based on user groups user rights with different levels are defined in the user administration of SIMATIC WinCC flexible.
- SIMATIC Logon provides the connection between the Windows user groups and the SIMATIC WinCC flexible user groups.
- If the network connection is failed, the central user management is assumed by the local user management. Thereby a predefined local emergency user can be used for maintenance of operation. SIMATIC Logon users (central users), which are already logged on, are still active until logoff.

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".

<sup>6</sup> From SIMATIC Logon V1.4.1 (V1.4 SP1)

## 2.2 Technological solution for audit trail

Audit trail are particularly important in situations in which users can create, modify or delete data during normal operation for standardized process documentation in electronic form. SIMATIC WinCC flexible supports the requirement for audit trail of operations actions, which are GMP relevant by recording such actions in an audit trail log file. The GMP relevant data is defined by the client based on the applicable legal guidelines.

We distinguish between changes made during production or runtime phase from changes made during the offline or configuration phase.

### Runtime phase

The relevant data to be tracked in the audit trail during runtime can be configured on the engineering system. The required information such as object name, old value, new value, date and time stamp, as well as user ID and optionally the reason for the change is saved.

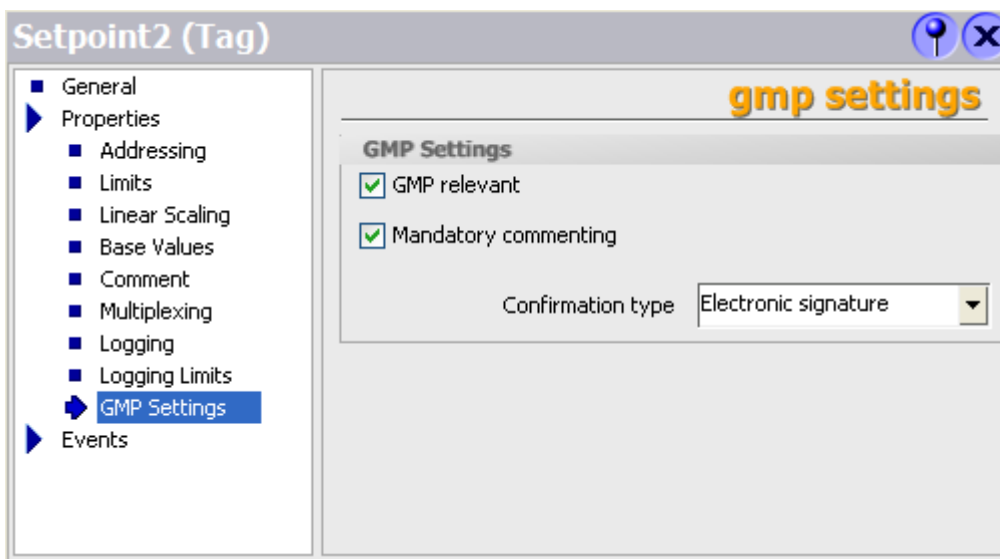


Figure 3: A variable is defined as GMP relevant so that an audit trail entry is created each time the user changes a value

The audit trail is saved as a csv-file or as a Unicode capable txt-file. An integrated algorithm automatically forms a checksum for each record and enables the user to detect manual changes of the records.

### Configuration phase

The WinCC flexible option ChangeControl enables the tracking of changes in WinCC flexible projects such as archives, alarm display and graphics, definition of access rights. The project versions are fully reproducible and can be rolled back. The respective project version can also be identified in the audit trail of the runtime.

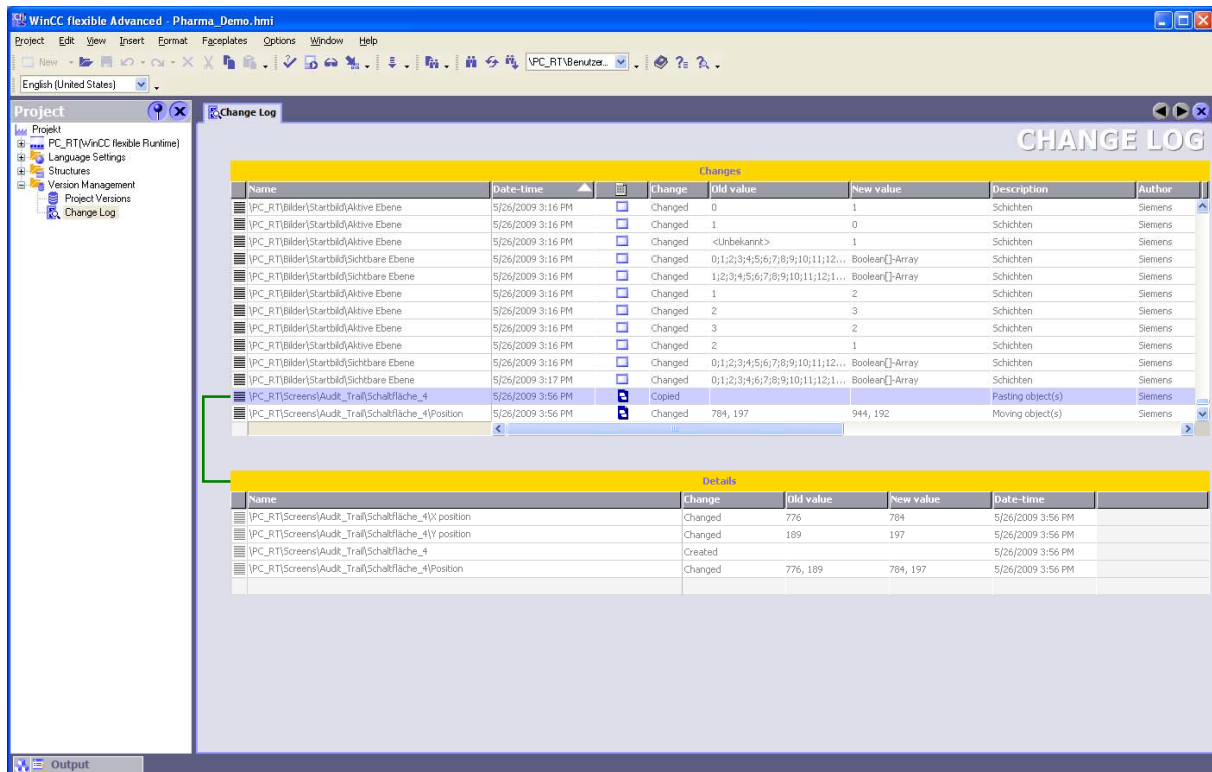


Figure 4: Change log which records the the modified configuration in a log file

## 2.3 Technological solution for data archiving and retrieval

### Process data

Process data (messages, process values) can be stored locally in csv- or in Unicode capable format or also as a binary file. For PC-projects ODBC-databases (e.g. MS SQL-Server) are also supported for storage. These process data can be archived for longtime storage via data transfer from mobile storage devices to the network. This can be configured to be driven manually, by time or by a process trigger. All longtime storage devices are acceptable, which are supported by Windows.

Recipe data records (parameter) are managed in an internal format by the system and can be exported or imported in csv-format if desired.

In case of long-term-archiving the data can be displayed with WinCC Audit Viewer, with a spreadsheet or with a text editor.

### Audit trail

The audit trail of operator actions during the runtime phase are recorded as an endless archive in the audit trail. Driven by time, process or storage capacity, these data are buffered to a local storage device (e. g. CF card), and then transferred via the network. From there, archiving to other storage media like CD or DVD is possible. The audit trail data can be displayed and printed with the WinCC Audit Viewer.

To protect data integrity of process data as well as audit trail data, the text based file formats can be provided with a checksum algorithm. Manipulation of data can be detected by means of a detection algorithm or the WinCC Audit Viewer. Thus, data integrity is assured.

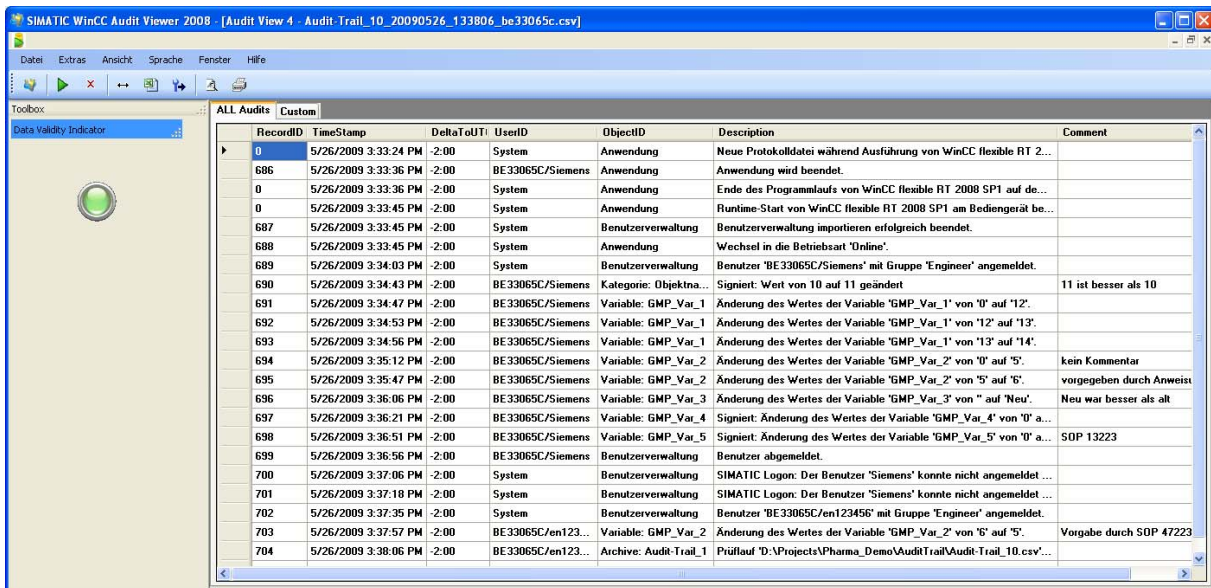


Figure 5: The Audit Viewer displays the audit trail and confirms with the green signal lamp that the audit trail has not been manipulated

## 2.4 Technological solution of electronic signatures

SIMATIC WinCC flexible supports electronic signatures for user actions. Which variables may require an electronic signature upon changes is specified during the configuration phase. The user can sign electronically by confirming the intended action with entering his password. In this way the electronic signature is saved in the audit trail along with the user name, the action performed and an additional comment. The comment can be configured as optional or mandatory for each object.

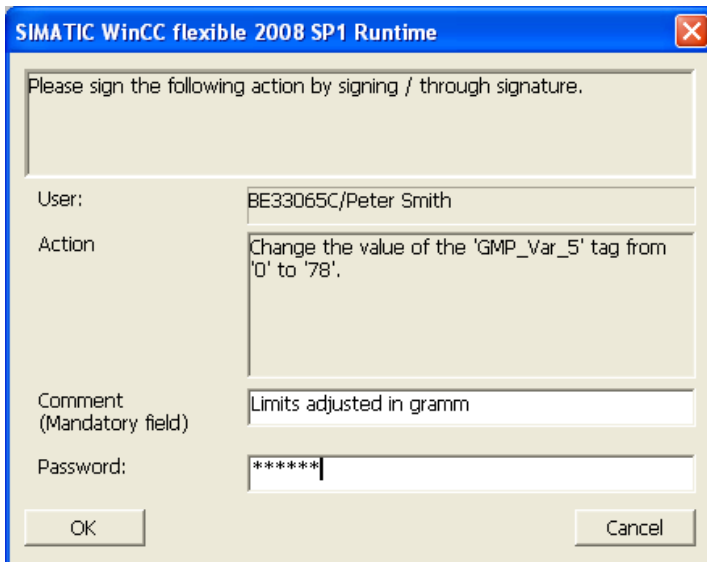


Figure 6: The modification of a tag value is signed electronically, taking into account the mandatory comment.

### 3 Evaluation List for SIMATIC WinCC flexible

The following checklist for a system assessment originates from a document of ISPE / PDA<sup>7</sup>

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 policies. The rules and standards always relate to the customer specific application that was implemented with SIMATIC WinCC flexible. 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 establish system life cycle (SLC) methodology, e.g as described in the GAMP guidelines.</p> <p>SIMATIC WinCC flexible 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>This is done by creating an entry in the audit trail for operator actions.</p> <p>The Audit Viewer displays available data records. The data to be logged in the audit trail are labeled during configuration by the "GMP-relevant" setting. For each data record a checksum is calculated and integrated in the audit trail. In this way manipulation to the audit trail can be detected. The required information for each record is recorded in a log file. The saved information includes the object name, the old value, new value, date and time stamp, as well user ID and optionally the reason for the change.</p> <p>Manipulation on process data (messages, values, recipes) can also be detected, because for these data a checksum is also available.</p> <p>Changes within the configuration of SIMATIC WinCC flexible can be tracked with the option ChangeControl.</p>

<sup>7</sup> 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 1	Is the system capable of producing accurate and complete copies of electronic records on paper?	<p>Yes.</p> <p>Alarms and messages, recipes and the audit trail can be printed during runtime.</p> <p>Additional these data as well as the process values can be transferred as a text file with checksum to a network resource and are then available to other applications for printing.</p>
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?	<p>Yes.</p> <p>Both process data (process value, messages, and recipes) and audit trails are generated as text based files and can be saved to a network resource.</p>
11.10(c)	Are the records readily retrievable throughout their retention period?	<p>Yes.</p> <p>The system uses resources available over a network to save the data over time.</p> <p>From there 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.</p> <p>Clients should also specify the retention periods and define procedures for archiving, backup and retrieval of electronic records.</p>
11.10(d)	Is system access limited to authorized individuals?	<p>Yes.</p> <p>All options of the Windows user management are active when the central user management of SIMATIC Logon is being used.</p> <p>With local user management only authorized individuals can log on to the system using their user ID and password. In this case the local runtime security settings are applied (see section 2.1 Technological solution for access security).</p> <p>The client should ensure, that only individuals who have a legitimate reason to use the system should be granted physical access to the system (e.g. HMI devices, engineering system).</p> <p>Because this requirement is virtually the same as 11.10(g), it is generally interpreted to refer to both physical access and logical access,</p>
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?	<p>Yes.</p> <p>The audit trail is secure within the system and cannot be changed by a user.</p> <p>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.</p>
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)?	<p>Yes.</p> <p>For process data, which are modified via the user interface the old and the new value are recorded in the audit trail. Process data which are electronically recorded cannot be modified by the user via the user interface.</p>

Paragraph/ detail	Questions / requirements	Comments
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 availability is ensured by logging in a separated text based file.
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. A specific sequence of operator actions can be realized by configuring the application accordingly.
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. SIMATIC WinCC flexible provides local user management with user groups, authorizations and users. It thereby regulates the management of system access as well as individual authorizations. The use of an electronic signature requires password input. Central user management can be implemented with SIMATIC Logon (see 11.10 (d)).
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 flexible devices can be configured so that special input of data / commands can only be performed from a dedicated workstation or from a group of dedicated workstations. All other devices then have only read-access right at the most.
11.10(i)	Is there documented training, including in-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?	Customers are responsible for providing procedural controls.
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?	Customers are responsible for providing procedural controls.

### 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. We recommend using SIMATIC WinCC flexible for operation in closed systems.

Paragraph/ detail	Questions / requirements	Comments
11.30 detail 1	Is data encrypted?	SIMATIC WinCC flexible has been designed for operation in closed systems. For operation in open systems, the “open path” of the data transfer should be secured by means of commercially available standard tools.
11.30 detail 2	Are digital signatures used?	SIMATIC WinCC flexible has been designed for operation in closed systems. For operation in open systems, the “open path” of the data transfer should be secured by means of commercially available standard tools.

### 3.3 Signed electronic records

See also section 2.4 “Technological solution of electronic signatures”

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 also include the following information: a) 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 records?	Yes. The information mentioned above are part of the audit trail and can be displayed and printed.
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. The electronic signature is part of the signed record within the audit trail. It is protected against change by the integrated checksum.

### 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 when SIMATIC Logon is used. It is not possible to define two users with the same user ID within the workgroup / domain.  If local user management is used, the uniqueness of the user ID and the combination of user ID and password are ensured by SIMATIC WinCC flexible.  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 the 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 respectively SIMATIC WinCC flexible identifies the person with two distinct components: 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)	When signing is performed the user ID of the logged on users is always given by the system. The password must be entered for each signing.
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?	The user ID is always given by the system and only the password component must be entered.
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.

Paragraph/ detail	Questions / requirements	Comments
11.200 (a)(3)	Would an attempt to falsify an electronic signature require the collaboration of at least two individuals?	<p>Yes.</p> <p>It is not possible to falsify an electronic signature during signing.</p> <p>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.</p> <p>Unauthorized using of user ID / passwords (failed logon attempts) is detected immediately and recorded.</p> <p>An attempt of falsification by the administrator once a record is saved would result in a change to its checksum, and the falsification would be detected.</p> <p>In addition, the customer needs procedural controls that prevent the disclosure of passwords.</p>

### 3.4.2 Electronic signature (biometric)

Paragraph/ detail	Questions / requirements	Comments
11.200(b)	Has it been shown that biometric electronic signatures can be used only by their genuine owner?	Biometric signature procedures are currently not supported by SIMATIC WinCC flexible.

### 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?	<p>See 11.100(a).</p> <p>The customer is responsible for creating procedural controls.</p>
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 creating procedural controls.
11.300(b) detail 2	Do passwords periodically expire and need to be revised?	<p>Yes.</p> <p>A password expires after a specified number of days and cannot be reused for a specified number of generations.</p>

Paragraph/ detail	Questions / requirements	Comments
11.300(b) detail 3	Is there a procedure for recalling identification codes and passwords if a person leaves or is transferred?	<p>Yes.</p> <p>Using SIMATIC Logon for central user management in conjunction with the MS Windows security system user accounts can be disabled.</p> <p>If the local user management of SIMATIC WinCC flexible is used, user access cannot be disabled or locked. But, a user group without any active user rights can be created, and inactive users assigned to it. Thus, user data are still available in the system without the user being able to do any unauthorized action in the system.</p> <p>The customer is responsible for creating procedural controls.</p>
11.300(c)	Is there a procedure for electronically disabling an identification code or password if it is potentially compromised or lost?	<p>Yes.</p> <p>The user can changed his password at any time if there is any suspicion of a breach of security. Passwords can be reset by administrators at any time if they are forgotten. A user ID can be "disabled" by organizational measures, such as described under 11.200(b) detail 3.</p>
11.300(d) detail 1	Is there a procedure for detecting attempts at unauthorized use and for informing security?	<p>Yes.</p> <p>Failed access attempts are recorded in the audit trail and can be identified and traced there.</p> <p>The user account is blocked after a specified number of unauthorized attempts.</p> <p>In addition, the customer is responsible for providing appropriate organizational measures.</p>
11.300(d) detail 2	Is there a procedure for reporting repeated or serious attempts at unauthorized use to management?	<p>The customer is responsible for providing appropriate organizational measures.</p>

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

Para-graph/ 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 flexible.
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 flexible.
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 flexible.
11.300(e) detail 1	Is there initial and periodic testing of tokens and cards?	Not applicable for pure software products like SIMATIC WinCC flexible.
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 flexible.

A5E02629496-01

**Siemens AG**  
Industry Sector  
Industry Automation  
VMM Pharma  
76181 KARLSRUHE  
GERMANY

pharma.aud@siemens.com  
[www.siemens.com/simatic-wincc-flexible](http://www.siemens.com/simatic-wincc-flexible)