SIEMENS

Compliance Response
21 CFR Part 11
SIMATIC WinCC V6.0

SIEMENS AG
Automation and Drives Group

Competence Center Chemical, Pharmaceutical Industry
D-76187 Karlsruhe, Federal Republic of Germany
Email: pharma@siemens.com
Fax: +49 (721) 595 7171

November 2003

Introduction

On August 20, 1997, the rule 21 CFR Part 11 “Electronic Records; Electronic Signatures” (ER / ES) became effective. The implementation of this rule is mandatory if ER/ES are applied. However, 21 CFR Part 11 applies only to records that are required to be maintained according to FDA regulations (as defined by predicate rules), or to records submitted to the FDA in electronic form. Several guidance and interpretation documents by the FDA (“Guidance for Industry”), the “GAMP Special Interest Group”, etc. are available. Furthermore traditional paper documents and handwritten signatures, or a mixture of both can still be used.

The intent of the rule is to facilitate introduction of electronic technology in manufacturing and production. Part 11 was created to give common sense guidelines on how to do in electronic form what was previously done on paper.

To help our users, Siemens as a supplier of Supervisory Control and Data Acquisition (SCADA) Systems, evaluated its systems according to the requirements of 21 CFR Part 11. In this paper the results of the assessment of the SCADA System "SIMATIC WinCC V6" are published.

SIMATIC WinCC V6.0 in combination with additional administrative and procedural controls, to be defined by the user, enables a full 21 CFR Part 11 compliance.

Siemens’ recommendations for architectural layout, system setup and configuration will facilitate system users to achieve compliance.

FDA requirements were originally applied in the Pharmaceutical industry, and meanwhile increasingly introduced in other industries such as Fine Chemicals and Food & Beverage.

The rule is open to interpretation therefore this document addresses common interpretation. The interpretation is expected to change over time and the compliance response will be reissued to reflect the changes. If the interpretation of the rule implemented by an individual organization differs from the enclosed, please contact the Competence Center Chemical and Pharmaceutical Industry in Karlsruhe, Germany for additional information.

This document consists of the following parts –the first part shows the requirements of Part 11 in short, the second gives WinCC’s answers to the main technological requirements, the third is a filled-out questionnaire list of the “GAMP Special Interest Group”.

1. The requirements of 21 CFR Part 11 in short

21 CFR Part 11 states that the risk of falsification, misinterpretation and change without leaving evidence are higher with electronic records and electronic signatures than paper records and handwritten signatures, and therefore specific controls are required.

“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.”

“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.”

Requirement	Description
Validation	Computer systems must be validated to ensure accuracy, reliability and consistency with intended performance.
Audit Trails	Systems must provide secure, computer-generated, time stamped audit trails to record actions that create, modify or delete electronic records.
Record Retention, Protection, Reproducibility and Retrievability	Systems must have 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

Requirement	Description
	electronic form.
Document Controls	Controls must exist over access to, revision of, distribution of, and use of documentation for system operation and maintenance.
Access Security	Systems must limit access to only authorized, qualified personnel. Special security measures must be provided within open systems, such as encryption for systems that can be accessed by outsiders.
Electronic Signature	Systems must provide measures to ensure that use of electronic signatures is limited to only genuine owners and that attempted use by others is detected and promptly recorded. Non-biometric systems must employ two distinct identification mechanisms (user-ID/password). Both user-ID and password must be entered before a signing session and at least the password is entered at each subsequent signing during 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 by ordinary means. 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.

2. WinCC´s answers to 21 CFR Part 11

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

- Access Security,
- Audit Trail,
- Archiving and Retrieval
- Electronic Signature

Technological solution for Access Security

Access Management with the “SIMATIC Logon” tool based on MS-Windows security is used to fulfill the requirements on access management:
- Based on user groups, user rights are defined in the WinCC "User Administration”.
- Individual users and their assignment to Windows user groups are defined in the Windows’ “User Administration” tool.
- With the SIMATIC Logon tool, the link between the Windows user groups and the WinCC user groups is established.

In this way, the following requirements on access management are fulfilled:
- Central administration of users (creating, blocking, unblocking, assigning to groups)
- Unique user-ID and combination of user-ID and password
- Setting access rights to groups and users
- Plant area dependent access and authorization levels
- Password aging: the user is forced to change his/her password after a preset time, password can be reused only after “n” generations
- The system can force the user to define a new password at the first log in
- User is automatically blocked after x erroneous login attempts and can only be unblocked by the administrator
- Automatic logout after pre-configurable idle time of keyboard or mouse
- Built in interface to support the implementation of electronic signature
- Login and logout – without system or application shutdown
- Log-functions of administrator actions regarding access management, online actions: login, logout (manual), logout (automatic), wrong user-ID, wrong password, user is blocked after a configurable number of consecutive erroneous password attempts, user changes his password

The “SIMATIC Logon“ tool in combination with procedures (for example clarifying the responsibility and access of the system users) fulfills the requirements of 21 CFR Part 11 regarding access security.

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”. If there is an "open path", then this path can be secured by using standard tools.

Technological solution for Audit Trail

Audit trails are particularly important where the system users are expected to create, modify, or delete regulated records during normal operation. In many cases an electronic record is stored and archived without changing it. In these cases, no audit trail is required and the electronic record is secured by WinCC itself (e.g. Access Security). In some cases where an audit trail is required, the requirements of the new FDA Guidance[1] regarding the implementation of the audit trail by a technical solution or other means is a user specific decision. Siemens as automation supplier offers a technological solution for audit trail which is described below.

We distinguish changes during the production / runtime phase of the system from changes which are made during the offline / configuration phase

Configuration phase

Configuration:
The tool " WinCC Audit" enables audit trail of changes of the WinCC configuration (e.g. archive, alarm, and graphic configuration, set up of access rights, etc.). The function “Document Control” of WinCC Audit allows full check in, check out, delete, rollback, and recovery of application documents (e.g. graphics screens, project functions or report layouts) and user documents. A secure database retains binary encoded copies of all past document revisions.

User administration changes:
Changes within the user administration (e.g. creating new users, blocking users etc.) are recorded by the Windows audit trail. For this purpose, the Windows Event Log should be configured accordingly.

Runtime phase

Process Data:
Process Data (e.g. tag logging data, alarms or operator messages) are stored without the ability to be changed by the operator.

Operational changes:
Changes during production / runtime, which are made by the operator on the WinCC SCADA System, are recorded in the message archive. Here a complete audit trail, recording all changes (set points, parameters, alarm acknowledgement, etc.), is made.

Technological solution for Archiving and Retrieval

WinCC offers a scalable archiving concept. This concept offers two archiving options: local WinCC archives or alternatively a central archive which can be configured according to the users’ needs. Furthermore, long term archiving through data export is possible.

WinCC offers standard interfaces to other archiving tools (Siemens or third party)

Retrieval can be achieved by standard WinCC Controls or by additional Option Packages (e.g. Dat@Monitor, Connectivity Pack). The WinCC Add-on PM Quality can further facilitate compliance in specific applications (e.g. batch processes, archiving and retrieval).

[1] Guidance for Industry. Part 11, Electronic Records; Electronic Signatures – Scope and Application, August 2003

Technological solution for Electronic Signature

Within WinCC, SIMATIC Logon is used as an interface (API) for an external electronic signature module. The electronic signature is executed through SIMATIC Logon. As identification mechanisms the input of user-ID and password is verified.

3. Evaluation List for WinCC

The following system assessment checklist for evaluating WinCC is taken from the document which has been developed by the GAMP Special Interest Group: “Complying with 21 CFR Part 11, Electronic Records and Electronic Signatures”[2].

The system assessment checklist involves all requirements not only those which can be fulfilled by technological solutions. Some of the requirements of 21 CFR Part 11 have to be fulfilled by the implementation of corresponding procedures by the user. The requirements of 21 CFR Part 11 always apply to the final user specific application which has been realized with WinCC V6.0. Therefore, the answers given below can only be valid if procedural and administrative controls are defined and adhered to.

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**	**Question / Requirement**	**Comments**
11.10(a) detail 1	Is the system validated ?	The user is responsible for the validation of the applications. The validation should follow an established system life cycle (SLC) methodology, e.g. as described in the current GAMP Guideline[3]. The validation of the application can be supported by Siemens during projects. WinCC has been developed according to Siemens’ Quality Management system (ISO 9001 certified) and includes validation supporting functions as defined in the NAMUR Recommendation NE72.
11.10(a) detail 2	Is it possible to discern invalid or altered records ?	Yes. An audit trail is generated upon any operating event (e.g. the operator changes set points, alarms limits, control modes, etc.). All relevant changes are recorded including date/time stamp, user-ID, old value/new value and explanatory text. Unauthorized changes are prevented by the system through access security. Changes within the configuration of WinCC can be tracked using WinCC Audit.
11.10(b) detail 1	Is the system capable of producing accurate and complete copies of records on paper ?	Yes. WinCC provides complete printouts of process data, alarms and messages.

[2] 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
[3] GAMP 4 Guide for Validation of Automated Systems; ISPE

Paragraph / **detail**	**Question / Requirement**	**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 data, alarms and messages including audit trail can be exported in electronic form and can be viewed with WinCC or the option Dat@Monitor. The WinCC option Audit allows export of Audit Trail records to Microsoft Excel, PDF format (if installed) or CSV files.
11.10(c)	Are the records readily retrievable throughout their retention period ?	Yes. Users are responsible for defining archiving strategies (retention periods, backup and recovery, archiving and retrieval). WinCC records can be archived e.g. on CD / MOD. The archived records can be viewed either using the tool Dat@Monitor or by restoring the records to WinCC[4].
11.10(d)	Is system access limited to authorized individuals ?	Since this requirement is virtually the same as 11.10(g) these are generally interpreted to refer to physical and logical access respectively. The user should ensure that only persons who have a legitimate business requirement to use the system have physical access to the system (e.g. server, systems console).
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 secured within the system and cannot be changed by a user. Changes during production will be audit trailed by the system itself and contain the information with time-stamp, user-ID or process source and action.
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 still available within the database. After changes have been made to electronic records such as reports, set points, the previous information is stored in the audit database of WinCC Audit and can be viewed by the WinCC option Audit Viewer.
11.10(e) detail 3	Is an electronic record's audit trail retrievable throughout the record's retention period ?	Yes. The audit trails (configuration and runtime) are retrievable throughout the record's retention period (see 11.10(c) concerning user's responsibility).
11.10(e) detail 4	Is the audit trail available for review and copying by the FDA ?	Yes. WinCC Audit allows export of Audit Trail records to Microsoft Excel, PDF format (if installed) or CSV files.
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) ?	A required sequence of operator actions can be forced by appropriate configuration (e.g. to require confirmation and verification).

[4] There is a known problem in WinCC V6.0 with respect to the visualization of trends during summer/winter time switchover. This problem is limited to the visualization and does not affect the recorded data. For more details see www.ad.siemens.com/support.

Paragraph / **detail**	**Question / Requirement**	**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 tool is layered on MS-Windows security. User-ID and password are used. Herewith, central user management for creating, blocking, and unblocking users with individual access rights is provided. Changes within the user administration are recorded in the Windows event log. In addition the user should define how access is limited to authorized individuals only (e. g. who has access to which object or function) 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 stations can be engineered so that special input of data / commands can be done only from a dedicated station or from a group of stations. The other stations then have only read-access rights or none. The system enforces validity checks because the stations have to be logged on 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 a wide range of standard and application specific training courses. The user is responsible for initiating and planning of these.
11.10(j)	Is there a written policy that holds individuals fully accountable and responsible for actions initiated under their electronic signatures ?	Users are responsible to provide procedural controls.
11.10(k) detail 1	Is the distribution of, access to, and use of systems operation and maintenance documentation controlled ?	Users are responsible to provide 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 ?	The user should define adequate change control procedures for operational and maintenance documentation.

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 be assessed against the requirements of this section additionally. We assume that WinCC is used by users who have full access control over the ER / ES system of WinCC.

Paragraph / detail	Question / Requirement	Comments
11.30 detail 1	Is data encrypted ?	WinCC in itself is a closed system and does not provide data encryption. In case of data transfer via an “open path”, there are standardized tools on the market to encrypt the records in order to make the "open path" secure.
11.30 detail 2	Are digital signatures used ?	WinCC does not provide a digital signature functionality. There are standardized tools on the market that enable digital signing of records.

Signed Electronic Records

See chapter 3
(Technological solution for Electronic Signature)

Paragraph / detail	Question / Requirement	Comments
11.50 detail 1	Do signed electronic records 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)	Within WinCC, SIMATIC Logon is used as an interface (API) for an external electronic signature module. The electronic signature is executed through SIMATIC Logon. As identification mechanisms the input of user-ID and password is verified. The printed user-ID of the signer, date, time and meaning of signing can be readily captured within the WinCC electronic record.
11.50 detail 2	Is the information above shown on displayed and printed copies of the electronic record ?	Above mentioned information can be printed and displayed as part 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 ?	Once an electronic record is signed, it can be stored in the WinCC message archive. This message cannot be cut, copied, changed or deleted. External access to the database is password-protected. In addition it is recommended to apply file access restrictions to the database by means of the Windows security features.

Electronic Signature (General)

Paragraph / detail	Question / Requirement	Comments
11.100(a) detail 1	Are electronic signatures unique to an individual ?	The external electronic signature module must ensure uniqueness of electronic signature to an individual. The electronic signature is using the user-ID and the password. The uniqueness of the user-ID and the combination of user-ID and password will be managed by SIMATIC Logon which is based on MS Windows security. It is not possible to define a user with the same user-ID within a workgroup / domain.

Paragraph / detail	Question / Requirement	Comments
11.100(a) detail2	Are electronic signatures ever reused by, or reassigned to, anyone else ?	The user has to ensure and is responsible that user-ID are never reassigned to anyone else. The SIMATIC Logon enforces, that each individual has his own unique identification.
11.100(b)	Is the identity of an individual verified before an electronic signature is allocated ?	Users' responsibility. They have to provide administrative controls.

Electronic Signature (Non-biometric)

	Question / Requirement	Comments
11.200 (a)(1)(i)	Is the signature made up of at least two components, such as an identification code and password, or an id card and password ?	Yes. The SIMATIC Logon tool identifies the person by 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)	Depending on the configuration, the user-ID and password can be requested for the first signing, and just the password for subsequent signings.
11.200 (a)(1)(iii)	If signings are not done in a continuous session, are both components of the electronic signature executed with each signing ?	This can be done through login / logoff sequences. Each signing can force the user to enter two components (user-ID plus password).
11.200 (a)(2)	Are non-biometric signatures only used by their genuine owners ?	Users are responsible to provide procedural controls.
11.200 (a)(3)	Would an attempt to falsify an electronic signature require the collaboration of at least two individuals ?	There is no possibility 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 creates the user-ID and defines an initial password, the system forces the user to change his password during first login. Unauthorized use of user-ID and passwords are detected immediately and recorded. In addition the user should provide procedures that prevent the disclosure of passwords.

Electronic Signatures (Biometric)

Paragraph / detail	Question / Requirement	Comments
11.200(b)	Has it been shown that biometric electronic signatures can be used only by their genuine owner ?	Third party tools can be connected via SIMATIC Logon. The integrity of such a solution should be specifically assessed.

Controls for Identification Codes and Passwords

If tokens, cards or other devices bearing or generating identification code or password information are used on this system for electronic signatures, then the system must be assessed against the requirements in this section.

Paragraph / detail	Question / Requirement	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 ?	Users are responsible to provide 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 policy settings. Password aging does not influence the previous use (records, signatures).
11.300(b) detail 3	Is there a procedure for recalling identification codes and passwords if a person leaves or is transferred ?	Users are responsible to provide procedural controls.
11.300(c)	Is there a procedure for electronically disabling an identification code or password if it is potentially compromised or lost ?	The system allows disabling of identification codes and passwords. However, it is the user's responsibility to put the adequate procedure in place.
11.300(d)	Is there a procedure for detecting attempts at unauthorized use and for informing security ?	Non authorized attempts are logged within the MS-Windows security log. The user account will be locked after a specified number of unauthorized attempts. In addition users are responsible to provide procedural controls.
11.300(d)	Is there a procedure for reporting repeated or serious attempts at unauthorized use to management ?	Users are responsible to provide procedural controls.
11.300(e) detail 1	Is there initial and periodic testing of tokens and cards ?	Users are responsible to provide procedural controls.
11.300(e) detail 2	Does this testing check that there have been no unauthorized alterations ?	Users are responsible to provide procedural controls.

Siemens is committed to continued development, supporting pharmaceutical applicants to comply with the GMP regulations.