SIEMENS

SIMATIC

SIMATIC WinCC Open Architecture (OA) V3.13
Electronic Records / Electronic Signatures (ERES)

Compliance Response

Edition 03/2015

Answers for industry.

SIEMENS

Compliance Response

Electronic Records / Electronic Signatures (ERES)

for SIMATIC WinCC Open Architecture (OA) V3.13

SIEMENS AG

VSS Pharma

D-76187 Karlsruhe, Germany

E-mail: pharma@siemens.com

March 2015

Table of Contents

Introduction

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

Accordingly regulatory bodies defined criteria under which electronic records and electronic signatures will be considered being as reliable and as trustworthy as paper records and handwritten signatures executed on paper. These requirements have been set forth by the US FDA in 21 CFR Part 11[1] (in short: *Part 11*) and by the European Commission in Annex 11 to chapter 4 of the EU GMP Guideline[2] (in short: *Annex 11*).
Because requirements on electronic records and electronic signatures are always tied to a computerized system being in a validated state, both regulations also include stipulations on validation and life-cycle of the computerized system.

Application of *Part 11* and *Annex 11* (or their corresponding implementation in national legislation) is mandatory for the use of electronic records and electronic signatures. However, these regulations are only valid within their defined scope.
The scope of both regulations is defined by the regional market the finished pharmaceutical is distributed to, and by whether or not the computerized systems and electronic records are used as a part of GMP-regulated activities (see Part 11.1[1] and Annex 11 Principle[2]).

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

To help its clients, Siemens as supplier of SIMATIC WinCC OA evaluated version 3.13 of the system with regard to these requirements and published its results in this Compliance Response. Due to its level of detail, this analysis is based on the regulations and guidelines mentioned above.

SIMATIC WinCC Open Architecture (OA) V3.13 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 regulated company). Such measures and controls are mentioned in chapter 3 of this document.

This document is divided into three parts: chapter 1 provides a brief description of the requirement clusters, while chapter 2 introduces the functionality of SIMATIC WinCC OA V3.13 as means to meet those requirements. Chapter 3 contains a detailed system assessment on the basis of the single requirements of the according regulations.

[1] 21 CFR Part 11 Electronic Records; Electronic Signatures, US FDA, March 20th 1997

[2] Volume 4 Good Manufacturing Practice Medicinal Products for Human and Veterinary Use / Annex 11: Computerised Systems, European Commission / EudraLex, June 30th 2011

1 The Requirements in Short

Annex 11 and Part 11 take into account that the risk of manipulation, misinterpretation and changes without leaving a visible trace is higher with electronic records and electronic signatures, than with conventional paper records and handwritten signatures. Furthermore the means to restrict access to electronic records to authorized individuals are very different to those required to restrict access to paper records. Additional measures are required for such reasons.

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.

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. Since electronic signatures are also considered being electronic records by themselves, all requirements on electronic records are applied to electronic signatures too.

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

Requirement	Description
Life Cycle and Validation of Computerized Systems	Computerized systems used as a part of GMP-related activities must be validated. The validation process should be defined using a risk-based approach. It should cover all relevant steps of the lifecycle and must provide appropriate documented evidence. The system’s functionality should be traceable throughout the lifecycle by being documented in specifications or a system description. A formal change control procedure as well as an incident management should be established. Periodic evaluation should confirm that the validated state of the system is being maintained.
Suppliers and Service Providers	Since competency and reliability of suppliers and service providers are considered as key factors, the supplier assessment should be chosen using a risk-based approach. Formal agreements should exist between the regulated user and these 3rd parties, including clear responsibilities of the 3rd party.
Data Integrity	Under the requirements of both regulations electronic records and electronic signatures must be as reliable and trustworthy as paper records. The system must provide the ability to discern altered records. Built-in checks for the correct and secure handling of data should be provided for manually entered data as well as for data being electronically exchanged with other systems. The system’s ability to generate accurate and complete copies is essential for the use of the electronic records for regulated purposes, as well as the accessibility, readability, and integrity of archived data throughout the retention period.
Audit Trail, Change Control Support	Besides recording changes to the system as defined in the lifecycle, both regulations require that changes on GMP-relevant data are being recorded. Such an audit trail should include information on the change (before / after data), the identity of the operator, a time stamp, as well as the reason for the change.

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

2 Meeting the Requirements with SIMATIC WinCC Open Architecture (OA)

The Siemens recommendations for the system architecture, conception, and configuration will assist system users in achieving compliance. For additional information and assistance see the SIMATIC WinCC OA Online Help.

The requirements explained in chapter 1 can be supported by the system as follows.

2.1 Life Cycle and Validation of Computerized Systems

Although *Annex 11* in 1992 and *Part 11* in 1997 underlined that a computerized system should be subject to validation, it was not until the 2011 revision of *Annex 11,* that a comprehensive set of criteria for the validation of the system and its life-cycle had been introduced.

Nonetheless the requirements to validate a computerized system and to keep it in a validated state had long been a part of regulations other than *Part 11* and *Annex 11*. This was the motivation for the ISPE[3] to publish practical guidance like the Baseline Guides[4], the GAMP 5[5] guide as well as the GAMP Good Practice Guides.

Thus the systems life-cycle as well as the approach to validation should be defined considering the guidance from the GAMP 5 guide. The guide also includes a number of appendices for life-cycle management, system development and operation of computerized systems.
Since most pharmaceutical companies already have a validation methodology for computerized systems as a part of their process landscape, it is preferable to setup the systems life-cycle and validation according to these.

2.2 Suppliers and Service Providers

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

[3] ISPE; International Society of Pharmaceutical Engineers, http://www.ispe.org

[4] Baseline® Pharmaceutical Engineering Guides for New and Renovated Facilities, Volume 1-7, ISPE

[5] GAMP 5 – A Risk-Based Approach to Compliant GxP Computerized Systems, ISPE, 2008

2.3 Data Integrity

Data integrity is assured in the system by measures like access security, audit trail, data type checks, checksums, backup/restore, and archiving/retrieval, completed by system validation, appropriate procedures and training for personnel.

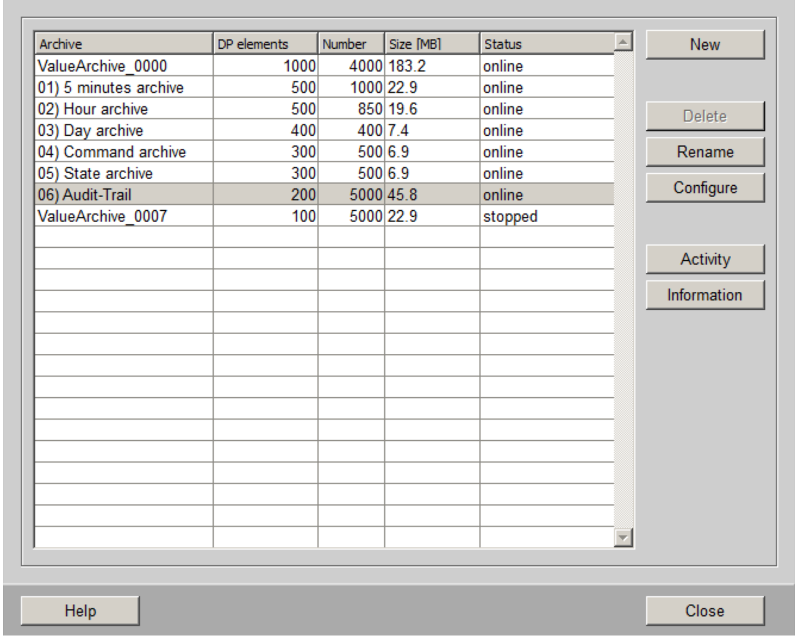
Data storage

WinCC OA can store data based on an ORACLE database which is recommended to fulfill the requirements.

Continuous archiving

Process data (messages, process values) and audit trails can be recorded and stored.

The number of archives may be defined as required. These should be generated and sorted thematically.

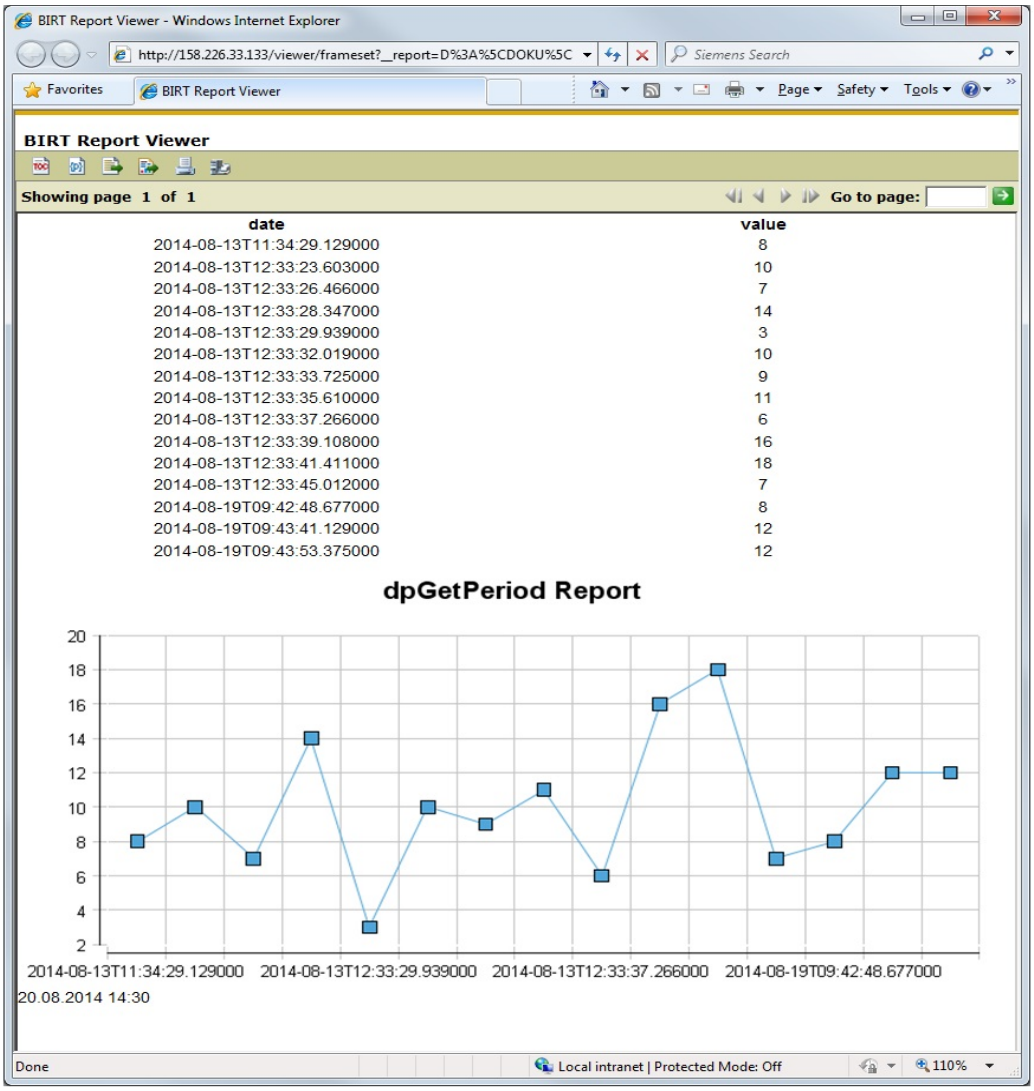


Archive	DP elements	Number	Size [MB]	Status
ValueArchive_0000	1000	4000	183.2	online
01) 5 minutes archive	500	1000	22.9	online
02) Hour archive	500	850	19.6	online
03) Day archive	400	400	7.4	online
04) Command archive	300	500	6.9	online
05) State archive	300	500	6.9	online
06) Audit-Trail	200	5000	45.8	online
ValueArchive_0007	100	5000	22.9	stopped

Figure 1: Overview of archives for a WinCC OA project

Batch-oriented archiving

The SIMATIC WinCC OA may be also used for batch-oriented data archiving. SIMATIC WinCC OA automatically manages the archives. To enable access to archived data one may use the SOAP interface of WinCC OA which can expose data via SSL encryption. Ready to use reporting templates based on ECLIPSE BIRT may be used.


BIRT Report Viewer - Windows Internet Explorer
http://158.226.33.133/viewer/frameset?__report=D%3A%5CDOKU%5C
Siemens Search
Favorites
BIRT Report Viewer
Page
Safety
Tools
BIRT Report Viewer
Showing page 1 of 1
Go to page:
20
18
16
14
12
10
8
6
4
2
2014-08-13T11:34:29.129000
2014-08-13T12:33:29.939000
2014-08-13T12:33:37.266000
2014-08-19T09:42:48.677000
Done
Local intranet | Protected Mode: Off
110%

date	value
2014-08-13T11:34:29.129000	8
2014-08-13T12:33:23.603000	10
2014-08-13T12:33:26.466000	7
2014-08-13T12:33:28.347000	14
2014-08-13T12:33:29.939000	3
2014-08-13T12:33:32.019000	10
2014-08-13T12:33:33.725000	9
2014-08-13T12:33:35.610000	11
2014-08-13T12:33:37.266000	6
2014-08-13T12:33:39.108000	16
2014-08-13T12:33:41.411000	18
2014-08-13T12:33:45.012000	7
2014-08-19T09:42:48.677000	8
2014-08-19T09:43:41.129000	12
2014-08-19T09:43:53.375000	12

dpGetPeriod Report

20.08.2014 14:30

Figure 2: Reporting example of a WinCC OA project

2.4 Audit Trail, Change Control Support

“Audit trails can be particularly appropriate when users are expected to create, modify, or delete regulated records during normal operation.” In other words, an audit trail is required for manually entered data and/or automatically recorded data, which have been modified or deleted by an operator.

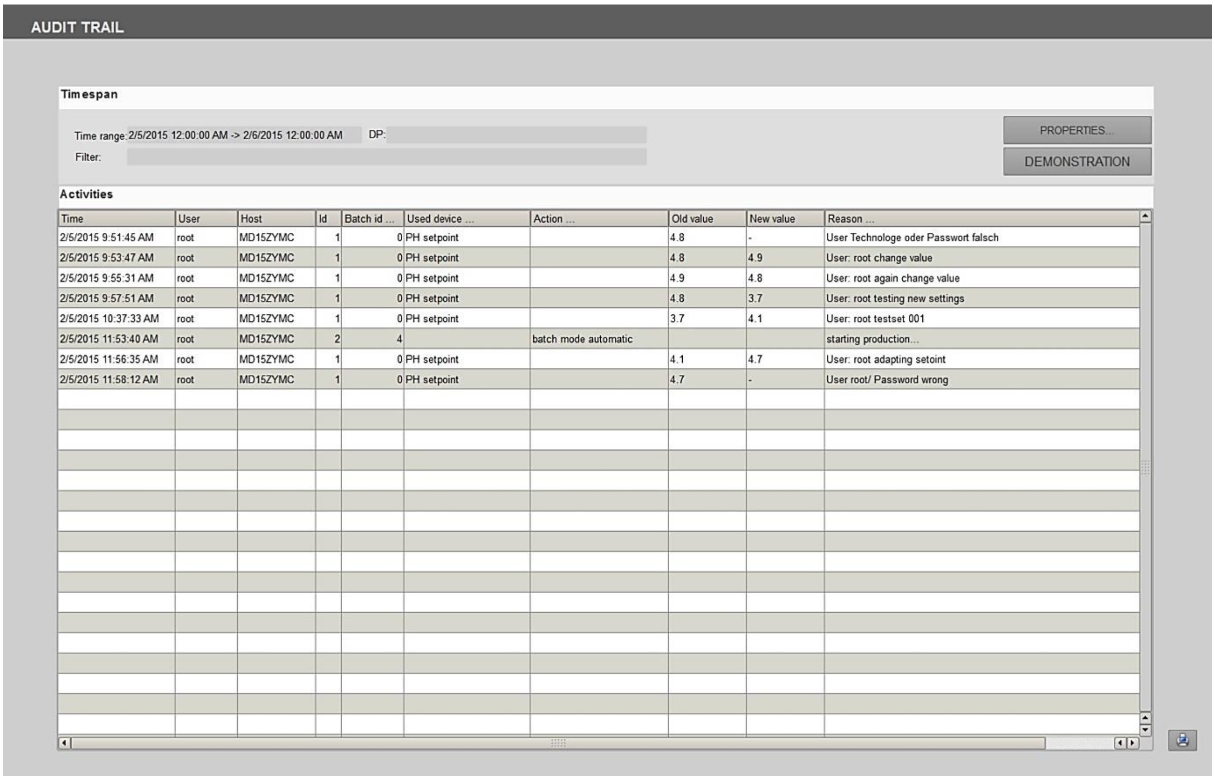
Audit trail during runtime operation

SIMATIC WinCC Open Architecture (OA) supports the requirement for audit trail of GMP relevant operations by recording such actions appropriately (who, what, when, and optionally why). And it provides adequate system security for such electronic records (e.g. access control). The GMP relevant data is defined by the regulated company based on the applicable regulatory requirements.

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

The audit trail is saved in the same way as the archive files. An integrated algorithm automatically forms a checksum for each record and enables the user to detect manual changes of the records.

Operator actions performed in SIMATIC WinCC Open Architecture (OA) can be recorded in an audit trail. The audit trail can be printed, exported, and archived.



Timespan

Time range: 2/5/2015 12:00:00 AM -> 2/6/2015 12:00:00 AM
DP:
Filter:

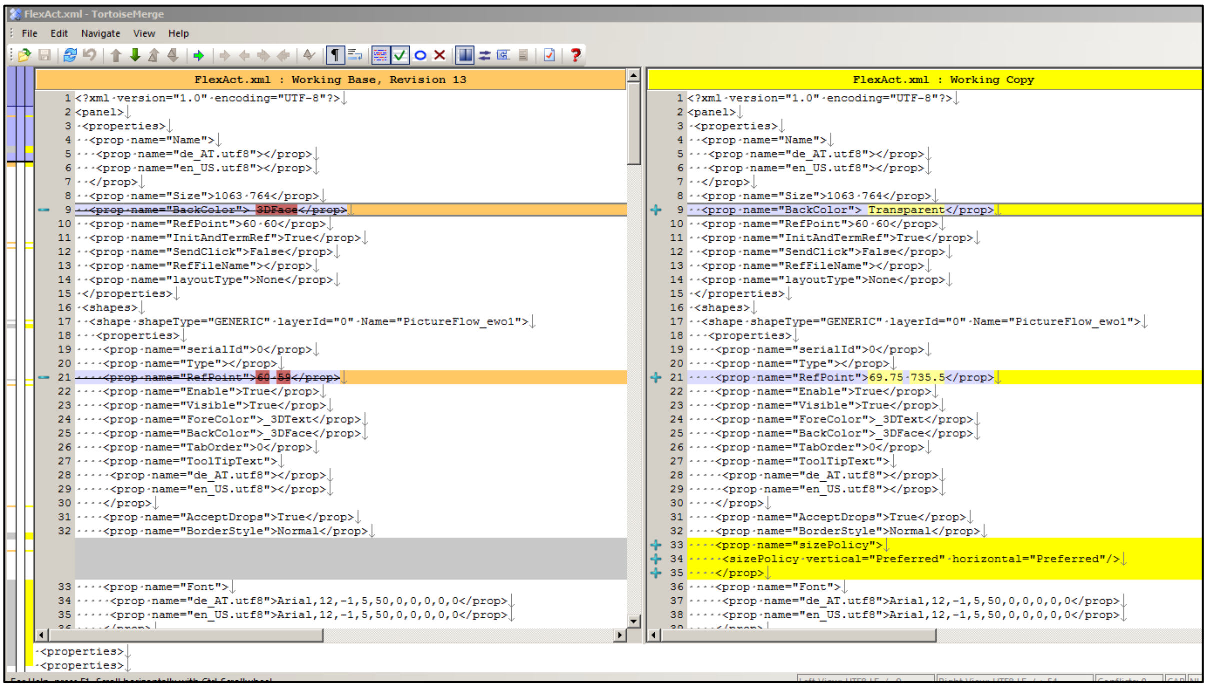
Activities

Time	User	Host	Id	Batch id ...	Used device ...	Action ...	Old value	New value	Reason ...
2/5/2015 9:51:45 AM	root	MD15ZYMC	1	0	PH setpoint		4.8	-	User Technologe oder Passwort falsch
2/5/2015 9:53:47 AM	root	MD15ZYMC	1	0	PH setpoint		4.8	4.9	User: root change value
2/5/2015 9:55:31 AM	root	MD15ZYMC	1	0	PH setpoint		4.9	4.8	User: root again change value
2/5/2015 9:57:51 AM	root	MD15ZYMC	1	0	PH setpoint		4.8	3.7	User: root testing new settings
2/5/2015 10:37:33 AM	root	MD15ZYMC	1	0	PH setpoint		3.7	4.1	User: root testset 001
2/5/2015 11:53:40 AM	root	MD15ZYMC	2	4		batch mode automatic			starting production...
2/5/2015 11:56:35 AM	root	MD15ZYMC	1	0	PH setpoint		4.1	4.7	User: root adapting setoint
2/5/2015 11:58:12 AM	root	MD15ZYMC	1	0	PH setpoint		4.7	-	User root/ Password wrong

Figure 3: Display of the audit trail

Configuration control

SIMATIC WinCC Open Architecture (OA) provides system functionalities and options to support the control of system configuration. This includes versioning of software elements and projects as well as backup/restore and comparison of different versions to support the corresponding procedures.



FlexAct.xml : Working Base, Revision 13

```
<?xml version="1.0" encoding="UTF-8"?>
<panel>
 <properties>
  <prop name="Name">
   <prop name="de_AT.utf8"></prop>
   <prop name="en_US.utf8"></prop>
  </prop>
  <prop name="Size">1063 764</prop>
  <prop name="BackColor"> 3DFace</prop>
  <prop name="RefPoint">60 60</prop>
  <prop name="InitAndTermRef">True</prop>
  <prop name="SendClick">False</prop>
  <prop name="RefFileName"></prop>
  <prop name="layoutType">None</prop>
 </properties>
 <shapes>
  <shape shapeType="GENERIC" layerId="0" Name="PictureFlow_ewo1">
   <properties>
    <prop name="serialId">0</prop>
    <prop name="Type"></prop>
    <prop name="RefPoint">60 59</prop>
    <prop name="Enable">True</prop>
    <prop name="Visible">True</prop>
    <prop name="ForeColor">_3DText</prop>
    <prop name="BackColor">_3DFace</prop>
    <prop name="TabOrder">0</prop>
    <prop name="ToolTipText">
     <prop name="de_AT.utf8"></prop>
     <prop name="en_US.utf8"></prop>
    </prop>
    <prop name="AcceptDrops">True</prop>
    <prop name="BorderStyle">Normal</prop>
    <prop name="Font">
     <prop name="de_AT.utf8">Arial,12,-1,5,50,0,0,0,0,0</prop>
     <prop name="en_US.utf8">Arial,12,-1,5,50,0,0,0,0,0</prop>
```

FlexAct.xml : Working Copy

```
<?xml version="1.0" encoding="UTF-8"?>
<panel>
 <properties>
  <prop name="Name">
   <prop name="de_AT.utf8"></prop>
   <prop name="en_US.utf8"></prop>
  </prop>
  <prop name="Size">1063 764</prop>
  <prop name="BackColor"> Transparent</prop>
  <prop name="RefPoint">60 60</prop>
  <prop name="InitAndTermRef">True</prop>
  <prop name="SendClick">False</prop>
  <prop name="RefFileName"></prop>
  <prop name="layoutType">None</prop>
 </properties>
 <shapes>
  <shape shapeType="GENERIC" layerId="0" Name="PictureFlow_ewo1">
   <properties>
    <prop name="serialId">0</prop>
    <prop name="Type"></prop>
    <prop name="RefPoint">69.75 735.5</prop>
    <prop name="Enable">True</prop>
    <prop name="Visible">True</prop>
    <prop name="ForeColor">_3DText</prop>
    <prop name="BackColor">_3DFace</prop>
    <prop name="TabOrder">0</prop>
    <prop name="ToolTipText">
     <prop name="de_AT.utf8"></prop>
     <prop name="en_US.utf8"></prop>
    </prop>
    <prop name="AcceptDrops">True</prop>
    <prop name="BorderStyle">Normal</prop>
    <prop name="sizePolicy">
     <sizePolicy vertical="Preferred" horizontal="Preferred"/>
    </prop>
    <prop name="Font">
     <prop name="de_AT.utf8">Arial,12,-1,5,50,0,0,0,0,0</prop>
     <prop name="en_US.utf8">Arial,12,-1,5,50,0,0,0,0,0</prop>
```

```
 <properties>
 <properties>
```

Figure 4: Comparison of a working base and a working copy

2.5 System Access, Identification Codes and Passwords

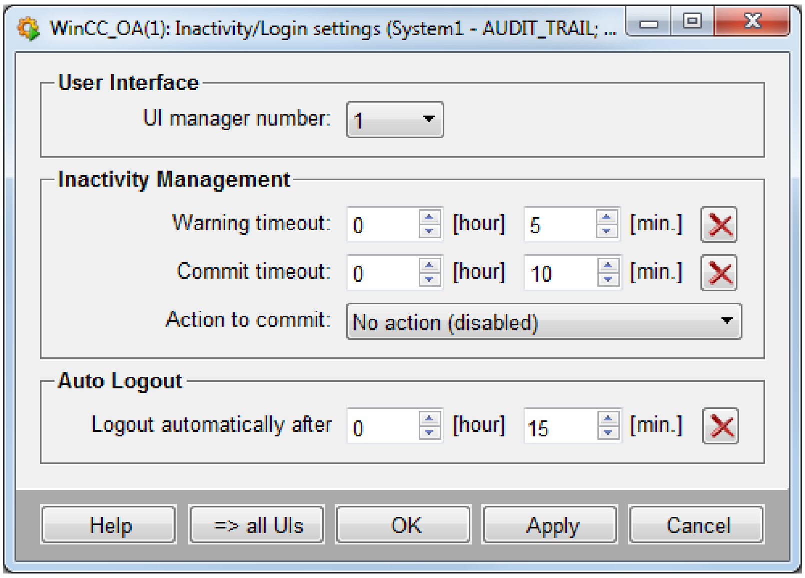
Users must be assigned the required access rights only, to prevent unauthorized access to the file system, the directory structures, and the system data and their unintended manipulation.

The requirements regarding access security are fully met in combination with procedural controls, such as those for “specifying the responsibility and access permission of the system users”.

SIMATIC WinCC OA complies with the requirements of IEC 61508 (*Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems*).

SIMATIC WinCC OA ensures the protection of electronic records by using user management either on Windows systems or using the Kerberos Service on Linux systems which enables:

- Use of unique user identification (user ID) in combination with a password (including language information).
- Definition of access rights for user groups.
- Password settings and 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.
- 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, failed login attempts, user blocked after several attempts to enter an incorrect password, and password change by user.



UI manager number: 1

Warning timeout: 0 [hour] 5 [min.]

Commit timeout: 0 [hour] 10 [min.]

Action to commit: No action (disabled)

Logout automatically after 0 [hour] 15 [min.]

Figure 5: Auto logoff Interface

Local user management

Local HMI panels are installed quite often without any connection to a network. Therefore, in SIMATIC WinCC Open Architecture (OA) local user management can be implemented, individual users and their assignment to user groups are then only known locally. Although it is strongly recommended to use a centralized user management either based on Microsoft Windows or based on the Kerberos Service while using Linux.

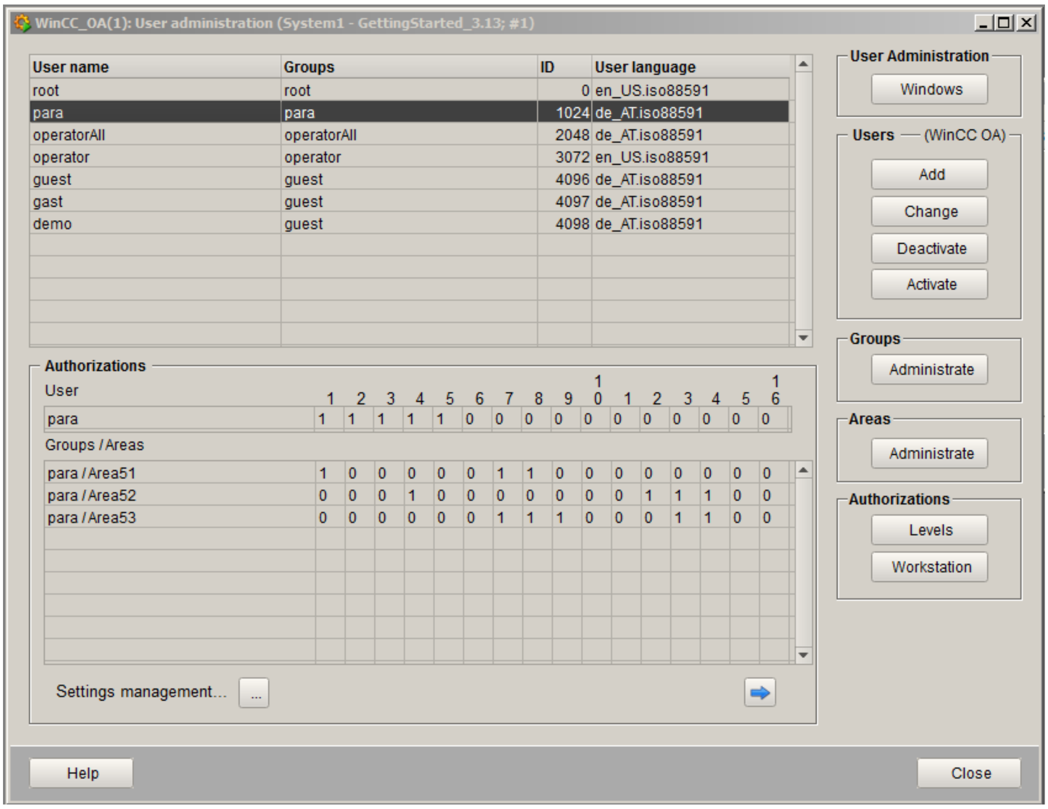
Individual users and their assignment to user groups are defined in the WinCC OA configuration.

Based on user groups, user rights with different levels are defined in the user administration for the particular SIMATIC WinCC Open Architecture (OA) system.

Centralized user management

A centralized user management based on Microsoft Windows or based on the Kerberos Service in a Linux environment is realized.

- Individual users and their assignment to user groups are defined in the User Access Control of Microsoft Windows or in the User Management of Linux.
- WinCC OA provides the link between those user groups and the user groups of the WinCC Runtime system.
- Based on user groups, user rights with different levels are defined in the user administration for the particular WinCC OA Runtime system.
- If the network connection is failed, WinCC OA falls into the so called safety case state and informs the user. Further login attempts will be refused. To avoid a single point of failure a backup domain controller is needed.



WinCC_OA(1): User administration (System1 - GettingStarted_3.13; #1)

User name	Groups	ID	User language
root	root	0	en_US.iso88591
para	para	1024	de_AT.iso88591
operatorAll	operatorAll	2048	de_AT.iso88591
operator	operator	3072	en_US.iso88591
guest	guest	4096	de_AT.iso88591
gast	guest	4097	de_AT.iso88591
demo	guest	4098	de_AT.iso88591

Authorizations

User	1	2	3	4	5	6	7	8	9	1 0	1	2	3	4	5	1 6
para	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0

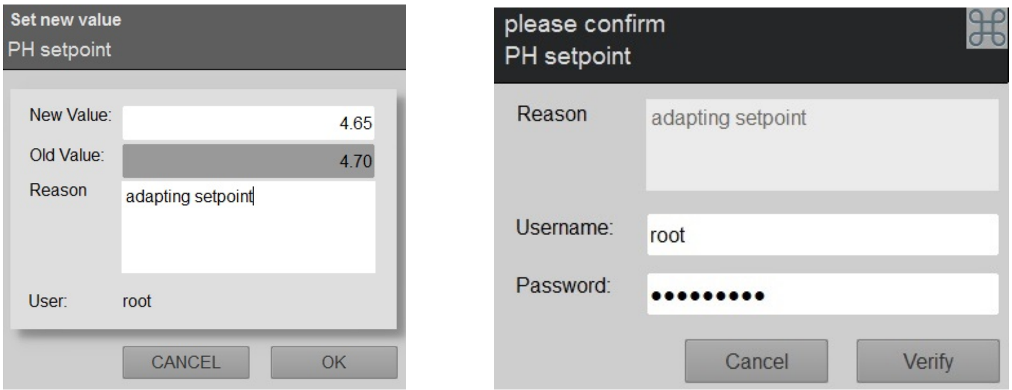
Groups / Areas

para / Area51	1	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0
para / Area52	0	0	0	1	0	0	0	0	0	0	0	1	1	1	0	0
para / Area53	0	0	0	0	0	0	1	1	1	0	0	0	1	1	0	0

Figure 6: Assignment of user rights to user groups and button to enable user management

2.6 Electronic Signature

SIMATIC WinCC Open Architecture (OA) provides functions for configuring an electronic signature. The electronic signature may be executed in a dialog. The variables which require an electronic signature upon changes are specified during the configuration phase. The user has to sign electronically by confirming the intended action with entering his password. Subsequently the electronic signature is saved in the audit trail along with the user name, time stamp, and the action performed. The comment can be configured as optional or mandatory for each operation.



Set new value
PH setpoint

New Value: 4.65
Old Value: 4.70
Reason: adapting setpoint
User: root

please confirm
PH setpoint

Reason: adapting setpoint
Username: root
Password: ●●●●●●●●●●

Figure 7: Electronic signature for modification of a tag value in SIMATIC WinCC Open Architecture (OA), including a mandatory comment.

3 Evaluation List for SIMATIC WinCC Open Architecture (OA)

The following list of requirements includes all regulatory requirements from 21 CFR Part 11 as well as from Annex 11. All requirements are structured in the same topics introduced in part 1 of this Compliance Response.

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

The *answers* include – if applicable – how the requirement is handled during the development of the product and which measures should be implemented during configuration and operation of the system. Furthermore the answers include references to the product documentation for technological topics and to the GAMP 5 guide for procedural controls that are already considered in the guide.

3.1 Life Cycle and Validation of Computerized Systems

The fundamental requirement that a computerized system, used as a part of GMP related activities, must be validated is extended by a number of newer Annex 11 requirements detailing expectations on a system's life cycle.

	Requirement	Reference	Answer
3.1.1	Risk management should be applied throughout the lifecycle of the computerized system.	Annex 11, 1	The R&D process for Siemens software products incorporates risk management accordingly. During the validation of a customer-specific application risk management should be ensured by the regulated user.
3.1.2	Validation of a system ensures the accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	21 CFR 11.10 (a)	Yes, the development of the software product (COTS, Commercial of the shelf software) is under the control of the Siemens QMS and the Product Lifecycle Management process. The regulated user should take appropriate measures to validate the application (see Annex 11, glossary), as well as maintaining its validated state.
3.1.3	Validation documentation covers relevant steps of the life cycle.	Annex 11, 4.1	Yes, the R&D process for the software product covers all relevant steps of the Software Development Life Cycle (SDLC). The responsibility for the validation of the application (see Annex 11, glossary) is with the regulated user.
3.1.4	A process for the validation of bespoke or customized systems should be in place.	Annex 11, 4.6	The validation process for customer-specific applications is under the responsibility of the regulated user. Nonetheless Siemens is able to offer support regarding validation activities.

	Requirement	Reference	Answer
3.1.5	Change management and deviation management are applied during the validation process.	Annex 11, 4.2	Yes, the R&D process for the software product includes change management, deviation management and fault corrections. The regulated user should ensure appropriate change management and deviation management (see GAMP 5, appendices M8, D5).
3.1.6	An up-to-date inventory of all relevant systems and their GMP functionality is available. For critical systems an up to date system description […] should be available.	Annex 11, 4.3	The regulated user should establish appropriate reporting, a system inventory as well as system descriptions (see GAMP 5, appendix D6).
3.1.7	User Requirements Specifications should describe required functions, be risk-based and be traceable throughout the life-cycle.	Annex 11, 4.4	Product Requirement Specifications are used during the R&D process. The regulated user should have the User Requirement Specification appropriately considered in the system's life cycle (see GAMP 5, appendix D1).
3.1.8	Evidence of appropriate test methods and test scenarios should be demonstrated.	Annex 11, 4.7	Ensuring the suitability of test methods and scenarios is an integral part of the SIMATIC product's R&D process and test planning. The regulated user should be involved to agree upon the testing practice (see GAMP 5, appendix D5) for the application.
3.1.9	Appropriate controls should be used over system documentation. Such controls include the distribution of, access to, and use of system operation and maintenance documentation.	21 CFR 11.10 (k)	During the development of the product the product's documentation is treated as being part of the product. Thus the documentation itself is under the control of the development process. The regulated user should establish appropriate procedural controls during development and operation of the production system (see GAMP 5, appendices M9 and D6).
3.1.10	A formal change control procedure for system documentation maintains a time sequenced record of changes.	21 CFR 11.10 (k) Annex 11. 10	During the development of the product changes are handled according to the development process. The regulated user should establish appropriate procedural controls during development and operation of the system (see GAMP 5, appendices M8 and O6).
3.1.11	Persons, who develop, maintain, or use electronic record/ electronic signature systems should have the education, training and experience to perform their assigned task.	21 CFR 11.10 (i)	Siemens' processes do ensure that employees have according training for their tasks and that such training is properly documented. Furthermore Siemens offers a variety of training courses for users, administrators and support staff.
3.1.12	Computerized systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP.	Annex 11, 11	The regulated user should establish appropriate procedural controls (see GAMP 5, appendices O3 and O8).

	Requirement	Reference	Answer
3.1.13	All incidents should be reported and assessed.	Annex 11, 13	SIMATIC WinCC Open Architecture (OA) offers functionalities to support reporting on different system levels. The regulated user should establish appropriate procedural controls (see GAMP 5, appendix O5).
3.1.14	For the availability of computerized systems supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown.	Annex 11, 16	The regulated user should appropriately consider the system in his business continuity planning (see GAMP 5, appendix O10).

3.2 Suppliers and Service Providers

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

	Requirement	Reference	Answer
3.2.1	When third parties are used, formal agreements must exist between the manufacturer and any third parties.	Annex 11, 3.1	The regulated user is responsible to establish formal agreements with suppliers and 3rd parties.
3.2.2	The competency and reliability of a supplier are key factors when selecting a product or service provider. The need for an audit should be based on a risk assessment.	Annex 11, 3.2 Annex 11, 4.5	The regulated user should assess its suppliers accordingly (see GAMP 5, appendix M2).
3.2.3	The regulated user should ensure that the system has been developed in accordance with an appropriate Quality Management System.	Annex 11, 4.5	The development of SIMATIC products follows the R&D process stipulated in Siemens' Quality Management System.
3.2.4	Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled.	Annex 11, 3.3	The regulated user is responsible for the performance of such reviews.
3.2.5	Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request.	Annex 11, 3.4	Matter and extent of the documentation affected by this requirement should be agreed upon by the regulated user and Siemens. The joint non-disclosure agreement should reflect this requirement accordingly.

3.3 Data Integrity

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

	Requirement	Reference	Answer
3.3.1	The system should provide the ability to discern invalid or altered records.	21 CFR 11.10 (a)	Feasible via the following functions: time stamping, quality bit, revisions, versioning for configuration and documents, and audit trail for operational entries.
3.3.2	For records supporting batch release it should be possible to generate printouts indicating if any of the data has changed since the original entry.	Annex 11, 8.2	Operational modification of data is recorded in the general audit trail and can be printed out in a report with internal or add-on functionality.
3.3.3	The system should provide the ability to generate accurate and complete copies of electronic records in both human readable and electronic form.	21 CFR 11.10 (b) Annex 11, 8.1	Yes. Accurate and complete copies can be generated in electronic portable document formats or on paper.
3.3.4	Computerized systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data.	Annex 11, 5	Yes. Depending on the type of data, such built-in checks include data type check, access authorizations, checksums, etc.
3.3.5	For critical data entered manually, there should be an additional check on the accuracy of the data.	Annex 11, 6	The system may implement built-in plausibility checks for data entry. In addition, an operator dialog can be realized as an additional check such as a four-eye principle.
3.3.6	Data should be secured by both physical and electronic means against damage.	Annex 11, 7.1	In addition to the system's access security mechanisms, the regulated user should establish appropriate security means like physical access control, backup strategy, limited user access authorizations, regular checks on data readability, etc. Furthermore the data retention period should be determined by the regulated user and appropriately considered in the users processes (see GAMP 5, appendices O3, O4, O8, O9, O11, O13). The WinCC OA security concept has to be considered.
3.3.7	Regular back-ups of all relevant data should be done.	Annex 11, 7.2	WinCC OA supports automated backups. The regulated user should establish appropriate processes for backup and restore (see GAMP 5, appendix O9).

	Requirement	Reference	Answer
3.3.8	Electronic records must be readily retrievable throughout the records retention period.	21 CFR 11.10 (c) Annex 11, 17	Yes. Data is generally stored in the database but can also be written in a user definable format into (single) files. WinCC OA provides automatic online backup, automatic external history storage and is, if desired, also capable of hot standby redundancy. As stated in point 3.3.7, procedural controls for Backup/Restore and Archiving/Retrieval should be established by the regulated user.
3.3.9	If the sequence of system steps or events is important, then appropriate operational system checks should be enforced.	21 CFR 11.10 (f)	Yes, e.g. allowances can be made for a specific sequence of operator actions by configuring the application accordingly.

3.4 Audit Trail, Change Control Support

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

	Requirement	Reference	Answer
3.4.1	The system should create a record of all GMP-relevant changes and deletions (a system generated “audit trail”). For change or deletion of GMP-relevant data the reason should be documented.	21 CFR 11.10 (e) Annex 11, 9	Yes. Changes during operation can be traced back by the system itself via audit trail and contain information with time stamp, user ID, old and new value, and comment. The audit trail is secure within the system and cannot be changed by a user. It can be made available and also be exported in electronic portable document formats.
3.4.2	Management systems for data and documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time.	Annex 11, 12.4	See point 3.4.1
3.4.3	Changes to electronic records shall not obscure previously recorded information.	21 CFR 11.10 (e)	Yes. Recorded information cannot be altered and is always available in the database.
3.4.4	The audit trail shall be retained for a period at least as long as that required for the subject electronic records.	21 CFR 11.10 (e) Annex 11, 9	Yes, this is technically feasible and must be considered in the application specific backup and restore process (cp. GAMP 5, appendices O9 and O13).
3.4.5	The audit trail should be available for review and copying by regulatory agencies.	21 CFR 11.10 (e)	Yes, see also point 3.4.1.

3.5 System Access, Identification Codes and Passwords

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

	Requirement	Reference	Answer
3.5.1	System access should be limited to authorized individuals.	21 CFR 11.10 (d) 21 CFR 11.10 (g) Annex 11, 12.1	Yes, SIMATIC WinCC Open Architecture (OA) has a built in fully featured access control system. This can be used either stand alone, connected with Microsoft Windows user administration or using the Kerberos Service in a Linux environment. All usual Windows features can be applied as well as the benefits of a centralized (domain-) administration. Nonetheless also procedural controls should be established by the regulated user, as described in GAMP 5, appendix O11.
3.5.2	The extent of security controls depends on the criticality of the computerized system.	Annex 11, 12.2	System security is a key factor during design and development of SIMATIC products. WinCC OA complies with IEC 61508. Nonetheless, since system security highly depends on the operating environment of each IT-system, these aspects should be considered in security management (see GAMP 5, appendix O11). Recommendations and support is given by Siemens' Industrial Security approach.
3.5.3	Creation, change, and cancellation of access authorizations should be recorded.	Annex 11, 12.3	Changes in the user access management may be recorded and should be subject to Change Control procedure.
3.5.4	If it is a requirement of the system that input data or instructions can only come from certain input devices (e.g. terminals), does the system check the validity of the source of any data or instructions received? (Note: This applies where data or instructions can come from more than one device, and therefore the system must verify the integrity of its source, such as a network of weigh scales, or remote, radio controlled terminals).	21 CFR 11.10 (h)	Yes. The devices can be configured so that special input data / commands can only be performed from a dedicated device, or from a group of dedicated devices. Besides the general log-in single operations, also additional log-ins or even an electronic signing of two different users of a certain user access level can be enforced.
3.5.5	Controls should be in place to maintain the uniqueness of each combined identification code and password, so that no individual can have the same combination of identification code and password as any other.	21 CFR 11.300 (a)	Yes. The uniqueness of the user ID is ensured either by the Microsoft Windows security system, by Linux system or by local user management of the WinCC OA device. It is not possible to define more than one user with the same user ID within a workgroup / domain.

	Requirement	Reference	Answer
3.5.6	Procedures are in place to ensure that the validity of identification codes is periodically checked.	21 CFR 11.300 (b)	The regulated user should establish appropriate procedural controls (see Good Practice and Compliance for Electronic Records and Signatures, Part 2).
3.5.7	Password should periodically expire and require to be revised.	21 CFR 11.300 (b)	Yes. Password aging can be configured using scripting or by configuring Windows or Linux security.
3.5.8	A procedure should be established for recalling identification codes and passwords if a person leaves or is transferred.	21 CFR 11.300 (b)	The regulated user should establish appropriate procedural controls (see Good Practice and Compliance for Electronic Records and Signatures, Part 2). A user account can be deactivated in Microsoft Windows security system or via Kerberos Service on Linux systems and local user management.
3.5.9	Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.	21 CFR 11.300 (c)	The regulated user should establish appropriate procedural controls (see Good Practice and Compliance for Electronic Records and Signatures, Part 2).
3.5.10	Measure for detecting attempts of unauthorized use and for informing security and management should be in place.	21 CFR 11.300 (d)	Yes. Unsuccessful attempts to use the system or to perform electronic signatures are recognized and can be logged using scripting or by configuring Windows security or via Kerberos Service Linux system. The regulated user should establish appropriate procedural controls to ensure a periodic review of security and access control information logs (see GAMP 5, appendix O8).
3.5.11	Initial and periodic testing of devices, such as tokens and cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.	21 CFR 11.300 (e)	Such devices are not part of WinCC OA portfolio, but might be integrated in the system via 3rd party tools. The regulated user should establish appropriate procedural controls (see Good Practice and Compliance for Electronic Records and Signatures, Part 2).

3.6 Electronic Signature

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

	Requirement	Reference	Answer
3.6.1	Written policies should be established, that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	21 CFR 11.10 (j) Annex 11, 14.a	The regulated user should establish appropriate procedural controls.
3.6.2	Signed electronic records should contain the following related Information: - The printed name of the signer - The date and time of signing - The meaning of the signing (such as approval, review, responsibility)	21 CFR 11.50 (a) Annex 11, 14.c	Yes. The username of the signer, date and time, and the meaning associated with the signature are stored in a database which is maintained by SIMATIC WinCC Open Architecture (OA).
3.6.3	The above listed information is shown on displayed and printed copies of the electronic record.	21 CFR 11.50 (b)	Yes. The items identified in point 3.6.2 are stored in the same database. Therefore they are subject to the same controls as electronic records.
3.6.4	Electronic signatures shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.	21 CFR 11.70 Annex 11, 14.b	Yes. The event records are maintained in a database and cannot be altered.
3.6.5	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	21 CFR 11.100 (a) 21 CFR 11.200 (a) (2)	Yes. The electronic signature uses the unique identifiers for user accounts. The re-use or re-assignment of electronic signatures is effectively prevented.
3.6.6	When a system is used for recording certification and batch release, the system should allow only Qualified Persons to certify the release of the batches and it should clearly identify and record the person releasing or certifying the batch.	Annex 11, 15	Electronic signatures are linked to an individual. The system allows strict determinations about which role and/or individual is allowed to perform a signature.
3.6.7	The identity of an individual should be verified before electronic signature components are allocated.	21 CFR 11.100 (b)	The regulated user should establish appropriate procedural controls for the verification of an individual’s identity before allocating a user account and/or electronic signatures.

	Requirement	Reference	Answer
3.6.8	When an individual executes one or more signings not performed during a single session, each signing shall be executed using all of the electronic signature components.	21 CFR 11.200 (a) (1) (ii)	Yes. Performing an electronic signature requires the user-ID as well as the user's password.
3.6.9	When an individual executes a series of signings during a single session, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one private electronic signature component.	21 CFR 11.200 (a) (1) (i)	Yes. Each signature consists of two components (user ID and password).
3.6.10	The use of an individual's electronic signature by anyone other than the genuine owner would require the collaboration of two or more individuals.	21 CFR 11.200 (a) (3)	Yes. It is not possible to falsify an electronic signature during signing or after recording of the signature. In addition, the regulated user needs procedures that prevent the disclosure of passwords.
3.6.11	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owner.	21 CFR 11.200 (b)	Standard tools of third-party manufacturers can be used to create biometric electronic signatures. The integrity of such solutions should be assessed separately.

3.7 Open Systems

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

	Requirement	Reference	Answer
3.7.1	To ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records additional measures such as data encryption are used.	21 CFR 11.30	SSL encryption for communication of managers to each other and to all clients is used consistently. Also the use of Kerberos is supported to allow secure communication over a non-secure network.
3.7.2	To ensure the authenticity and integrity of electronic signatures, additional measures such as the use of digital signature standards are used.	21 CFR 11.30	SIMATIC WinCC Open Architecture (OA) does not provide functionality for digital (encrypted) signatures.

Further information

E-Mail:
pharma@siemens.com

Internet:
www.siemens.com/pharma

Siemens AG
Industry Sector
Pharmaceutical and Life
Science Industry
76187 KARLSRUHE
GERMANY

Subject to change without prior notice
A5E35430010-AA

Siemens
Pharma Industry

www.siemens.com/automation