## SIMATIC WinCC V7.0

### GMP Engineering Manual

Guidelines for Implementing Automation Projects in a GMP Environment

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction, Table of Contents</td>
<td>1</td>
</tr>
<tr>
<td>Configuring in a GMP Environment</td>
<td>2</td>
</tr>
<tr>
<td>Requirements of Computer Systems in a GMP Environment</td>
<td>3</td>
</tr>
<tr>
<td>System Specification</td>
<td>4</td>
</tr>
<tr>
<td>System Installation and Configuration</td>
<td>5</td>
</tr>
<tr>
<td>Project Settings and Definitions</td>
<td>6</td>
</tr>
<tr>
<td>Creating Application Software</td>
<td>7</td>
</tr>
<tr>
<td>Support During Qualification</td>
<td>8</td>
</tr>
<tr>
<td>Operation, Service and Maintenance</td>
<td>9</td>
</tr>
<tr>
<td>System Updates and Migration</td>
<td></td>
</tr>
<tr>
<td>Index List</td>
<td></td>
</tr>
</tbody>
</table>
Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

<table>
<thead>
<tr>
<th><strong>DANGER</strong></th>
<th>indicates that death or severe personal injury will result if proper precautions are not taken.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>WARNING</strong></th>
<th>indicates that death or severe personal injury may result if proper precautions are not taken.</th>
</tr>
</thead>
</table>

| **CAUTION** with a safety alert symbol, indicates that minor personal injury can result if proper precautions are not taken. |
|---|---|

| **CAUTION** without a safety alert symbol, indicates that property damage can result if proper precautions are not taken. |
|---|---|

<table>
<thead>
<tr>
<th><strong>NOTICE</strong></th>
<th>indicates that an unintended result or situation can occur if the corresponding information is not taken into account.</th>
</tr>
</thead>
</table>

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by personnel qualified for the specific task in accordance with the relevant documentation for the specific task, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

| **WARNING** Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be adhered to. The information in the relevant documentation must be observed. |
|---|---|

Trademarks

All names identified by ® are registered trademarks of the Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.
Introduction

Purpose of this manual
This manual describes what is required from the pharmaceutical, regulatory viewpoint for Good Manufacturing Practice (GMP), of the computer system, its software and the procedure for configuring such a system. Practical examples are used to explain the relationship between requirements and implementation.

Target groups
This manual is intended for all plant operators, those responsible for system designs for specific industries, project managers and programmers, servicing and maintenance personnel who use the automation and process control technology in the GMP environment.

Basic knowledge required
Basic knowledge of SIMATIC WinCC is required to understand this manual. Knowledge of GMP as practiced in the pharmaceutical industry is also an advantage.

Disclaimer of liability
This manual contains instructions for system users and programmers for integrating SIMATIC WinCC into the GMP environment. It covers validation and takes into account special aspects such as the requirements of FDA 21 CFR Part 11.

We have checked that the contents of this document correspond to the hardware and software described. However, as deviations cannot be precluded entirely, we cannot guarantee complete accuracy of the information contained herein. The information in this document is checked regularly for system changes or changes to the regulations of the various organizations and necessary corrections will be included in subsequent issues. We welcome any suggestions for improvement and ask that they be sent to the I IA VMM Pharma in Karlsruhe (Germany).

Validity of the manual
The information in this manual applies to SIMATIC WinCC V7.0 incl. SP1. The components investigated are SIMATIC WinCC (CS/RT) in conjunction with the WinCC/CAS (Central Archive Server), SIMATIC Version Trail, WinCC/Audit, WinCC/Web Navigator, WinCC/DataMonitor options and the WinCC Premium Add-ons PM-CONTROL and PM-QUALITY. Refer to the catalog CA01 for information about the exact compatibility of SIMATIC WinCC V7.0 with the individual components. This catalog is available online at www.siemens.com/automation/ca01. A list relating to the compatibility of the various product versions can be accessed at http://support.automation.siemens.com/DE/view/en/21927773.

Position in the information landscape

The system documentation of the SIMATIC WinCC V7.0 HMI system is an integral part of the SIMATIC WinCC system software. It is available to every user as online help (HTML help) or as electronic documentation in Acrobat Reader format (PDF) as the "SIMATIC HMI Document Collection".

Structure of the manual

This manual supplements the existing SIMATIC WinCC manuals. The guidelines are not only useful during configuration, they also provide an overview of the requirements for configuration and what is expected of computer systems in a GMP environment.

The rules and guidelines, recommendations and mandatory specifications are explained, that represent the basis for configuration of computer systems.

All the necessary functions and requirements for hardware and software components are also described, which should make the selection of components easier.

The use of the hardware and software and how they are configured or programmed to meet the requirements is explained based on examples. More detailed explanations are available in the standard documentation.

Additional support

If this manual does not contain the answers to any questions you may have about how to use the products described, please contact your local Siemens representative.

Find your contact partner at:
http://www.siemens.com/automation/partner

A guide to the technical documentation of the various SIMATIC products and systems is available at:
http://support.automation.siemens.com/WW/view/de/4000024

The online catalog and online ordering system are available at:
http://mall.automation.siemens.com/

If you have questions on the manual, please contact I IA VMM Pharma

E-mail: pharma.aud@siemens.com

Further information about the products, systems and services from Siemens for the pharmaceutical industry can be found at:
http://www.siemens.com/pharma
Training centers

Siemens offers a number of training courses to familiarize you with the SIMATIC WinCC operator control and monitoring system. Please contact your regional training center or our main training center in 90327 Nuremberg, Germany, for details.

Internet:  http://www.sitrain.com

Technical support

You can contact technical support for all I IA&DT products

- by submitting the Support Request web form  
  http://www.siemens.com/automation/support-request

and the Center of Competence for WinCC in Mannheim at

-  WinCCAddon.automation@siemens.com

You will find more information about our technical support on the Internet at

http://www.siemens.de/automation/service

Online service & support

In addition to our pool of documentation, we offer you a comprehensive online knowledge base.

http://www.siemens.com/automation/service&support

There you will find:

- The newsletter that provides you with latest information relating to your product
- The right documents for you, using our Service & Support search engine
- A bulletin board in which users and specialists worldwide exchange their know-how
- Your local Siemens representative
- Information about on-site service, repairs and spare parts. Much more is available on the "Services" pages.
# Table of Contents

## Introduction

- Configuring in a GMP Environment
  - Regulations and Guidelines
  - Life Cycle Model
  - Responsibilities
  - Approval and Change Procedure
  - Risk-Based Approach

## Requirements of Computer Systems in a GMP Environment

- Categorization of Hardware and Software
- Test Effort Depending on the Categorization
- Project Change and Configuration Management
- Software Creation
- Access Protection and User Management
  - Applying access protection to a system
  - Requirements of user IDs and passwords
- Requirements of Electronic Records
- Electronic Signatures
- Audit Trail
- Reporting Batch Data
- Archiving Data
- Data Backup
- Retrieving Archived Data
- Clock Synchronization
- Use of Third-Party Components

## System Specification

- Specification of the Visualization Hardware
  - Selecting the hardware components
  - Hardware specification
- System and Network Security
- Specification of the Basic Software
  - Operating system
  - Basic software for user administration
  - Engineering software components
  - HMI level software components
  - Long-term archiving
  - Reporting
  - Availability and plant configuration
  - Interfaces to process data
### Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.4 SIMATIC Additional Software</td>
<td>28</td>
</tr>
<tr>
<td>3.4.1 Batch-oriented control with PM-CONTROL</td>
<td>28</td>
</tr>
<tr>
<td>3.4.2 Batch-oriented reporting with PM-QUALITY</td>
<td>29</td>
</tr>
<tr>
<td>3.4.3 Batch-based long-term archiving with PM-QUALITY</td>
<td>30</td>
</tr>
<tr>
<td>4 System Installation and Configuration</td>
<td>31</td>
</tr>
<tr>
<td>4.1 Installation of the Operating System</td>
<td>31</td>
</tr>
<tr>
<td>4.2 SIMATIC Installations</td>
<td>31</td>
</tr>
<tr>
<td>4.2.1 SIMATIC WinCC</td>
<td>31</td>
</tr>
<tr>
<td>4.2.2 SIMATIC Security Control</td>
<td>32</td>
</tr>
<tr>
<td>4.2.3 SIMATIC WinCC options</td>
<td>32</td>
</tr>
<tr>
<td>4.2.4 Setting up long-term archiving</td>
<td>32</td>
</tr>
<tr>
<td>4.3 Setting up User Administration</td>
<td>32</td>
</tr>
<tr>
<td>4.3.1 User administration on the operating system level</td>
<td>34</td>
</tr>
<tr>
<td>4.3.2 Security settings in Windows</td>
<td>35</td>
</tr>
<tr>
<td>4.3.3 Configuration of SIMATIC Logon</td>
<td>35</td>
</tr>
<tr>
<td>4.4 Administration of User Rights</td>
<td>36</td>
</tr>
<tr>
<td>4.5 Configuring Access Protection</td>
<td>37</td>
</tr>
<tr>
<td>5 Project Settings and Definitions</td>
<td>39</td>
</tr>
<tr>
<td>5.1 Startup Characteristics</td>
<td>39</td>
</tr>
<tr>
<td>5.2 Object-Oriented Configuration</td>
<td>40</td>
</tr>
<tr>
<td>5.2.1 Faceplate types</td>
<td>41</td>
</tr>
<tr>
<td>5.2.2 User objects</td>
<td>41</td>
</tr>
<tr>
<td>5.2.3 Screen window</td>
<td>41</td>
</tr>
<tr>
<td>5.2.4 Structure tag</td>
<td>41</td>
</tr>
<tr>
<td>5.2.5 Library of the Graphics Designer</td>
<td>42</td>
</tr>
<tr>
<td>5.2.6 Project functions in the form of scripts</td>
<td>42</td>
</tr>
<tr>
<td>5.3 Configuring Redundancy</td>
<td>43</td>
</tr>
<tr>
<td>5.4 Clock Synchronization</td>
<td>44</td>
</tr>
<tr>
<td>5.4.1 Concepts for time-of-day synchronization</td>
<td>45</td>
</tr>
<tr>
<td>5.4.2 Time synchronization Central Archive Server (CAS)</td>
<td>45</td>
</tr>
<tr>
<td>5.4.3 Time stamping</td>
<td>46</td>
</tr>
<tr>
<td>5.5 Configuration Management</td>
<td>47</td>
</tr>
<tr>
<td>5.6 Versioning Application Software</td>
<td>48</td>
</tr>
<tr>
<td>5.6.1 Versioning pictures in Graphics Designer</td>
<td>49</td>
</tr>
<tr>
<td>5.6.2 Versioning VB / C scripts</td>
<td>50</td>
</tr>
<tr>
<td>5.6.3 Versioning reports</td>
<td>52</td>
</tr>
<tr>
<td>6 Creating Application Software</td>
<td>53</td>
</tr>
<tr>
<td>6.1 Creating the Graphic User Interface</td>
<td>53</td>
</tr>
<tr>
<td>6.2 Creating Operator Input Messages</td>
<td>53</td>
</tr>
<tr>
<td>6.3 Electronic Signature</td>
<td>55</td>
</tr>
<tr>
<td>6.4 Audit Trail</td>
<td>56</td>
</tr>
<tr>
<td>6.4.1 Audit trail via WinCC Alarm Logging</td>
<td>56</td>
</tr>
<tr>
<td>6.4.2 Audit trail via WinCC/Audit</td>
<td>60</td>
</tr>
<tr>
<td>6.5 Recording and Archiving Data Electronically</td>
<td>51</td>
</tr>
<tr>
<td>6.5.1 Specifying the data to be archived</td>
<td>51</td>
</tr>
<tr>
<td>6.5.2 Setting up user archives</td>
<td>52</td>
</tr>
<tr>
<td>6.5.3 Recording and archiving</td>
<td>52</td>
</tr>
<tr>
<td>6.6 Reporting</td>
<td>64</td>
</tr>
<tr>
<td>6.6.1 Reporting with WinCC Report Designer</td>
<td>64</td>
</tr>
</tbody>
</table>
Table of Contents

6.6.2 Batch-oriented reporting with PM-QUALITY .......................................................... 66
6.7 Monitoring the System .................................................. 67
6.7.1 Diagnostics of communication connections .................................................. 67
6.7.2 System information channel ........................................ 68
6.7.3 Lifebeat monitoring ............................................... 68
6.8 Data Exchange with the Plant Management Level .............................................. 69
6.9 Connecting to a Web Client ............................................. 69
6.9.1 Setting up operator permissions on the WinCC server .................................. 70
6.9.2 Remote access via the network ..................................... 71
6.9.3 Web access to display data .......................................... 72
6.10 Interfaces to SIMATIC WinCC ........................................ 73
6.10.1 Interfacing SIMATIC WinCC flexible ........................................ 73
6.10.2 Interfacing SIMATIC S7 .............................................. 73
6.10.3 Interfacing third-party components .................................. 74

7 Support During Qualification ........................................................ 75
7.1 Qualification Planning ..................................................... 75
7.2 Qualification of the Hardware .......................................... 76
7.3 Qualification of the Software ............................................ 76
7.3.1 Software categorization according to GAMP Guide .................................. 77
7.3.2 Qualification of standard software .................................. 77
7.3.3 Qualification of the application software .................................. 79
7.4 Configuration Control .................................................. 79
7.4.1 Project versioning .................................................... 79
7.4.2 Change control of the configuration data .................................. 82
7.5 Backing Up the Operating System and SIMATIC WinCC .......................... 84

8 Operation, Service and Maintenance .............................................. 85
8.1 Operation and Monitoring .................................................. 85
8.2 Change Control during Operation ........................................ 85
8.3 System Recovery ........................................................ 86
8.4 Uninterruptible Power Supply (UPS) ........................................ 88

9 System Updates and Migration .................................................. 89
9.1 Updates, Service Packs and Hotfixes ........................................ 89
9.2 Migration of the Application Software ...................................... 90

Index List ................................................................................. 91
1 Configuring in a GMP Environment

Before configuring computer systems in a GMP environment, approved specifications must be available. Requirements contained in standards, recommendations, and guidelines must be observed when creating these specifications and when implementing and operating computer systems. This chapter deals with the most important sets of regulations and explains some of the basic ideas.

1.1 Regulations and Guidelines

The regulations, guidelines, and recommendations of various national and international agencies and organizations have to be taken into account when configuring computer systems requiring validation in the GMP environment. Where computer systems are involved, the following are of particular significance:

<table>
<thead>
<tr>
<th>Name (Originator)</th>
<th>Title</th>
<th>Validity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Annex 11 of the EU GMP Guide (European Commission)</td>
<td>Computerized systems</td>
<td>Binding directive within the European Union for implementation in relevant national legislation</td>
</tr>
<tr>
<td>GAMP5 (ISPE)</td>
<td>A Risk-Based Approach to Compliant GxP Computerized Systems</td>
<td>Guideline with worldwide validity as recommendation</td>
</tr>
</tbody>
</table>

1.2 Life Cycle Model

A central component of Good Engineering Practice (GEP) is the application of a recognized project methodology, based on a defined life cycle. The aim is to deliver a solution that meets the relevant requirements, known as the so-called risk-based approach.

GAMP5 Approach

The following schematic shows the general approach according to GAMP5 for developing computerized systems. It begins with the planning phase of a project and ends with the start of pharmaceutical production after the completion of the tests and reports.
The lifecycle approach illustrated here is called the generic model in GAMP5. With this as the basis, several examples of lifecycle models for a variety of "critical" systems with different stages of specification and verification phases are shown as examples.

Once production has started, the complete system life cycle continues until the product is taken out of service.

**Siemens Validation Manual**

Based on the recommendations of the GAMP Guide, Siemens has produced a "Validation Manual". This provides internal project teams with general information and concrete templates to help specify the validation strategy for a project. There are templates not only for project planning documents but also for the system specification and test documentation. In contrast to this GMP Manual, the Siemens Validation Manual is only for internal Siemens use.

**1.3 Responsibilities**

Responsibilities for the activities included in the individual life cycle phases must be defined when configuring computer systems in a GMP environment and creating relevant specifications. As this definition is usually laid down on a customer- and project-specific basis and requires a contractual agreement, it is recommended that the definition is integrated into the quality and project plan.

**See also**

- GAMP5 Guide, Appendix M6 "Supplier Quality and Project Planning"
1.4 Approval and Change Procedure

When new systems requiring validation are set up or when existing systems requiring validation are changed, the top priority is to achieve or retain the validated status. This assures traceability of all executed steps.

Before creating or modifying a system, it is therefore necessary to plan and document the pending steps in terms of functionality and time, and to obtain approval by the customer respectively by the plant operating company.

1.5 Risk-Based Approach

Both the US agency FDA ("cGMPs 21st Century", 2004) and the industry association ISPE/GAMP ("GAMP5", 2008 guide) recommend a risk-based approach to the validation of systems. This means that whether and to what extent a system will be validated depends on its complexity and its influence on the product quality.
2 Requirements of Computer Systems in a GMP Environment

This chapter describes the essential requirements which an automated system must meet in the GMP environment in terms of using computerized systems. These requirements must be defined in the specification and implemented during configuration. In general, proof of who has changed or performed what and when they have done it must always be recorded (the “why” is optional). The requirements of this task are implemented in various functions and described in the following chapters.

Note
This chapter describes the general requirements for computerized systems. How to meet the concrete requirements with a specific system is dealt with starting at chapter 3.

2.1 Categorization of Hardware and Software

Hardware categorization
According to the GAMP Guide, hardware components of a system fall into two categories “standard hardware components” (category 1) and “custom built hardware components” (category 2).

Software categorization
According to the GAMP Guide, the software components of a system are divided into various software categories. These include commercially available and preconfigured “standard” software products that are simply installed, configured software products, right through to custom applications (“programmed software”).

2.2 Test Effort Depending on the Categorization
The effort involved in validation (specifying and testing) is much greater when using configured and, in particular, customized products compared with the effort for standard products (hardware and/or software). The overall effort for validation can therefore be significantly reduced by extensive use of standard products.
2.3 Project Change and Configuration Management

All the supervised elements of a system should be identified by name and version and any changes made to them should be checked. The changeover to the operational procedure should be decided in good time.

The procedure includes, for example:

- Identification of the elements affected
- Identification of the elements by name and version number
- Change control
- Control of the configuration (storage, release, etc.)
- Periodic checks of the configuration

See also

- GAMP5 Guide, Appendix M8 "Project Change and Configuration Management"

2.4 Software Creation

Certain guidelines must be followed during software creation, which must be documented in the Quality and Project Plan (GEP idea). Software creation guidelines can be found in the GAMP Guide as well as the relevant standards and recommendations.

Validation effort when using typicals

While the validation of standard software only calls for the software name and version to be checked, customized software validation requires the entire range of functions to be checked and a supplier audit to be performed.

To keep validation work to a minimum, preference should be given to standardized function blocks during configuration (products, standard company components, standard project components). Customer-tailored typicals are created from standard function blocks and tested according to design specifications.

Identifying software modules/typicals

During software creation the individual software modules must be assigned a unique name, a version, and a short description of the module.

Changing software modules/typicals

Changes to software modules should be appropriately documented. Apart from incrementing the version identifier, the date and the name of the person performing the change should be recorded, when applicable with a reference to the corresponding change request/order.
2.5 Access Protection and User Management

To ensure that automated systems in the GMP environment are secure, such systems must be equipped with an access-control system. Access-control systems not only deny or permit users access to certain rooms, but can also protect systems against unauthorized access. Users are put into groups which are in turn used to manage user rights. Individual users can be granted access authorization in various ways:

- A combination of unique user ID and password - a description of the configuration can be found in chapter 2.5.2 “Requirements of user IDs and passwords”.
- Chip cards together with a password
- Biometric systems, for example finger print scanners

2.5.1 Applying access protection to a system

In general, actions that can be executed on a computer system must be protected. Depending on his or her particular field of activities, a user can be assigned various rights. Access to user administration should only be given to the system owner or to a very limited number of employees. Unauthorized access to recorded electronic data must also be prevented.

The use of an automatic logout functions is advisable and provides additional access security. This does not, however, absolve the user from the general responsibility of logging off when exiting the system. The automatic logout time should be agreed with the user and defined in the specification.

Note
Only authorized persons must be able to access PCs and the system. This can be ensured by using appropriate measures such as mechanical locks and hardware and software for remote access.

2.5.2 Requirements of user IDs and passwords

User ID

The user ID for a system must be of a minimum length defined by the customer and be unique within the system.

Password

When defining passwords, the minimum number of characters and the expiry period for the password should be defined. A password should generally comprise a combination of character with a minimum length and should also meet at least three of the criteria listed below.

- Use of uppercase letters
- Use of lowercase letters
- Use of numerals (0-9)
- Use of special characters

The configuration is described in chapter 4.3 “Setting up User Administration”. 
2.6 Requirements of Electronic Records

When using electronic records for relevant data, the following additional requirements apply:

- The system must be validated.
- Only authorized persons must be able to enter or change data (access protection).
- Changes to data or deletions must be recorded (audit trail).
- Relevant electronic records for long-term storage must be archived securely and kept available for their retention period.
- The initials and signatures required by the regulations must be implemented as electronic signatures.
- "Relevant" production steps / processes, "significant" interim stages and "major" equipment must be defined in advance by the person responsible from a pharmaceutical perspective; this definition is often process-specific.
- If an electronic manufacturing log is used, its structure and contents must match the structure and contents of the manufacturing formula / processing instructions. As an alternative, the manufacturing instructions and log can also be combined in one document.

See also

- EU GMP Guide Chapter 4.9
- 21 CFR Part 11 Electronic Records, Electronic Signatures

2.7 Electronic Signatures

Electronic signatures are computer-generated character strings, which act as legally binding equivalents to handwritten signatures.

Regulations concerning the use of electronic signatures are defined, for example, in US FDA 21 CFR Part 11.

Electronic signatures are of practical relevance, for example, when it comes to manual data input and operator intervention during runtime, approving process actions and data reports, and changing recipes.

Each electronic signature must be assigned uniquely to one person and must not be used by any other person.

Note

The FDA regulations including 21 CFR Part 11 must be satisfied in the manufacture of all pharmaceutical products and medical devices intended for the US market.
Conventional electronic signatures

If electronic signatures are used that are not based on biometrics, they must be created so that persons executing signatures must identify themselves using at least two identifying components. This also applies in all cases where a smart card replaces one of the two identification components. These identification components can, for example, be a user ID and a password. The identification components must be assigned uniquely and must only be used by the actual owner of the signature.

Electronic signatures based on biometrics

An electronic signature based on biometrics must be created in such a way that it can only be used by one person. If the person making the signature does so using biometric methods, one identification component is adequate.

Possible biometric recognition systems include systems for scanning a fingerprint or the iris of the eye.

2.8 Audit Trail

The audit trail is a control mechanism of the system that allows the tracking of all data entered or modified. A secure Audit trail is particularly important as regards the creation, modification, or deletion of GMP-relevant electronic records.

Such an audit trail must document all the changes or actions made along with the date and time. The typical content of an audit trail describes who changed what and when (old value / new value), as an option it may also include “why”.

2.9 Reporting Batch Data

Batch documentation is particularly important where the manufacture of pharmaceutical products and medical devices is concerned. Correctly created batch documentation is often the only documentary evidence that pharmaceutical manufacturers can provide in the context of product liability.

The components of batch documentation are as follows:

- Manufacturing formula / processing instructions and manufacturing log
- Packaging instructions and packaging log (from a pharmaceutical point of view, the packaging of the finished medicinal product is part of the manufacturing process)
- Test instructions and test log (relating to quality checks, for example analysis)

The manufacturing log (or packaging log) has a central significance here as defined below:

- The manufacturing log is always both product-related and batch-related.
- It is always based on the relevant parts of the valid manufacturing formula and processing instructions.
- It records all measurement and control procedures relevant to the process as actual values
- It compares these with the specified desired values
2.10 Archiving Data

Archiving means the permanent storage of electronic data and records in a long-term storage system.\(^1\)

The customer is responsible for defining procedures and controls relating to the retention of electronic data.

Based on predicate rules (GMP Guide, 21 CFR Part 210/211, etc.), the customer must decide how electronic data will be retained and, in particular, which data will be involved by this procedure. This decision must be founded on a sound and documented risk assessment, which also takes the relevance of the electronic data over the time period it is to be archived into account.

If logged data is migrated or converted, the integrity of that data must be safeguarded throughout the entire conversion process.\(^2\)

2.11 Data Backup

In contrast to the archiving of electronic data, data backups are used to create backup copies that allow the system to be restored if the original data or entire system is lost.\(^3\)

The backup procedure must include the periodic backup of volatile information to avoid total loss of data due to defective system components or inadvertent deletion of data. Backup procedures must be tested to ensure that data is saved correctly. Backup records should be labeled clearly and intelligibly and dated.\(^3\)

Data backups are created on external data carriers. The data carrier used should comply with the recommendations of the device manufacturer.

When backing up electronic data, the following distinctions are made:

- Backup of the installation, for example partition image
- Backup of the application
- Backup of archive data, for example process data

Here, particular attention is paid to the storage of data backup media (storage of the copy and original in different locations, protection from magnetic fields, and elementary damage).

2.12 Retrieving Archived Data

Archived/backed up data must be retrievable at all times. If the system is updated, care must be taken that the data transferred to archive prior to the update remains compatible.

---


\(^3\) "Electronic Records and Electronic Signatures Assessment". Chris Reid & Barbara Mullendore, PDA 2001.
2.13 Clock Synchronization

A uniform time reference (including a time zone reference) must be guaranteed within a system, to be able to assign an unequivocal time stamp for archiving messages, alarms etc.

Time synchronization is especially important for archiving data and analysis of faults. UTC (Universal Time Coordinated, defined in ISO 8601) is recommended as the time base for saving data. The time can be displayed in local time with a note regarding summer / winter time.

2.14 Use of Third-Party Components

If third-party components (hardware and software) are used, it must be confirmed that such components are compatible with the other components being used. In case of components being specifically tailored to individual customers a supplier audit should be performed in order to check the supplier and their quality management system.

See also

- GAMP5 Guide, Appendix M2 "Supplier Assessment"
3 System Specification

During the specification phase for a computer system, the system to be set up and its functionality are defined in as much detail as is required for setup. This also includes the selection of products, product versions/options, and system configurations.

### 3.1 Specification of the Visualization Hardware

With SIMATIC WinCC, you can implement a variety of different system configurations from single-user systems to multiple-user systems with a client/server structure.

- Single user system with complete operation and monitoring of a production process via a single PC
- Multiple-user system consisting of operator stations (WinCC clients) and one or more WinCC servers that supply the WinCC clients with data

Availability can be increased by setting up redundant systems.

### 3.1.1 Selecting the hardware components

The SIMATIC WinCC software can be installed on any standard PC that meets the minimum requirements for the hardware and software configuration. You will find details in the current SIMATIC HMI catalog ST 80.

For production plants in a GMP environment (for example, in food and beverages or pharmaceutical industry) Siemens has developed particularly rugged panel PCs with touch screens and stainless steel fronts specially for installation on the shop floor.
The SIMATIC WinCC software is available as a pure software package or in conjunction with a Panel PC as a complete HMI system.

A higher level of availability is achieved with the WinCC server’s redundant structure. All hardware components such as PC, screen, operator controls are set up in duplicate. If one system fails, the other automatically assumes functionality.

**Note**
We recommend using the approved hardware from the current SIMATIC HMI catalog ST80 since its compatibility has been checked by Siemens in system tests.

When PCs are installed in switching cabinets, make sure that suitable hardware components are used, for example remote kits.

### 3.1.2 Hardware specification

The Hardware Design Specification (acronym: HDS) describes the hardware architecture and configuration. The HDS should, for example define the points listed below. This specification is used later as a test basis for the IQ and OQ.

- Hardware overview diagram
- Network structure
- PC components for server and client
- Automation system with CPUs, I/O cards, etc.
- Field devices

The HDS can be recorded in the Functional Specification or in a separate document.

**Note**
The information in the hardware overview diagram and the naming of hardware components must be unequivocal. The designation for each hardware component may only occur once in the computerized system.

**See also**
- GAMP5 Guide, Appendix D3 "Configuration and Design"

### 3.2 System and Network Security

In modern SCADA systems, the boundaries between the office world and that of automation are increasingly disappearing. Automation solutions with connected WEB clients, MES connections, customized office networks and their office applications are growing in importance. To satisfy these demands and ensure as high a level of data security as possible, the planning and structure of networked WinCC automation solutions are highly important.

**See also**
- Manual "Security Concept PCS 7 and WinCC"
Measures to improve system security

SIMATIC WinCC offers several ways of improving system security. These include:

- Centralized user administration
- SIMATIC Security Control (SSC)
- SIMATIC NET SCALANCE S

SIMATIC Security Control

The SIMATIC Security Control application checks the settings in the MS Windows operating system in terms of the requirements for the SIMATIC software installed. Registry keys and DCOM settings are evaluated and exceptions put forward for the Windows firewall. The settings needed for WinCC are made automatically in the Windows operating system by clicking the "Accept" button. Documentation of the settings can be printed or saved in XML format.

SIMATIC Security Control ships with SIMATIC WinCC.

SIMATIC NET SCALANCE S

SCALANCE S security modules are at the heart of Siemens' ground-breaking security concept for protecting networks and data. The SCALANCE S protection function checks all data traffic to and from the cell.

With a combination of different security measures such as firewall, NAT/NAPT routers and VPN (Virtual Private Network) over IPsec tunnels, the SCALANCE S devices protect individual devices or even entire automation cells from:

- Data espionage
- Data manipulation
- Unauthorized access

See also

- Manuals of the SCALANCE family

3.3 Specification of the Basic Software

The software specification describes not only the application software but also the standard software components used in the system, for example by specifying the name, version number etc.

Commercially available standard software components include automation software components and software provided by third parties such as the operating system, Acrobat Reader, MS Office, etc.

From the available range of the WinCC system software, the following components will be discussed in this manual.
### 3.3.1 Operating system

You will find up-to-date information on operating system installation in the "Installation Notes" accompanying the software package.

### 3.3.2 Basic software for user administration

Access protection for SIMATIC WinCC system components and the WinCC Premium Add-ons is implemented with the SIMATIC Logon software. SIMATIC Logon supports a user management system based on Windows mechanisms that can be used both in workgroup and in a Windows domain. (see chapter 4.3 "Setting up User Administration")

See also
- SIMATIC Logon Configuration Manual

<table>
<thead>
<tr>
<th>Name</th>
<th>Brief Description</th>
<th>Additional license necessary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm Logging</td>
<td>Message archiving</td>
<td></td>
</tr>
<tr>
<td>Basic Process Control</td>
<td>Overview diagram and screen navigation, Clock synchronization</td>
<td></td>
</tr>
<tr>
<td>Configuration Tool</td>
<td>WinCC configuration using MS Excel</td>
<td></td>
</tr>
<tr>
<td>Graphics Designer</td>
<td>Editor for producing graphics</td>
<td></td>
</tr>
<tr>
<td>Project Duplicator</td>
<td>WinCC tool for copying/duplicating a WinCC project</td>
<td></td>
</tr>
<tr>
<td>Report Designer</td>
<td>Production of reports</td>
<td></td>
</tr>
<tr>
<td>SIMATIC Logon service</td>
<td>Interfacing to Windows user administration</td>
<td></td>
</tr>
<tr>
<td>SIMATIC Security Control</td>
<td>DCOM and firewall settings</td>
<td></td>
</tr>
<tr>
<td>Tag Logging</td>
<td>Process value archiving</td>
<td></td>
</tr>
<tr>
<td>User Administrator</td>
<td>User management in WinCC</td>
<td></td>
</tr>
<tr>
<td>Tag Management</td>
<td>Tag Management</td>
<td></td>
</tr>
<tr>
<td>WinCC/Audit</td>
<td>Central Audit Trail for recording operator actions during operations and changes in the project configuration</td>
<td>X</td>
</tr>
<tr>
<td>WinCC/ChangeControl</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WinCC/CAS</td>
<td>Central data archiving</td>
<td>X</td>
</tr>
<tr>
<td>Central Archive Server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WinCC/Connectivity Pack</td>
<td>External access to archives and messages</td>
<td>X</td>
</tr>
<tr>
<td>WinCC/DataMonitor</td>
<td>View of data via the web</td>
<td>X</td>
</tr>
<tr>
<td>WinCC/DowntimeMonitor</td>
<td>Recording and analysis of downtimes</td>
<td>X</td>
</tr>
<tr>
<td>WinCC/Redundancy</td>
<td>Redundant WinCC server</td>
<td>X</td>
</tr>
<tr>
<td>WinCC/Server</td>
<td>For the server in a server/client structure</td>
<td>X</td>
</tr>
<tr>
<td>WinCC/User Archives</td>
<td>Production of user archives</td>
<td>X</td>
</tr>
<tr>
<td>WinCC/Web Navigator</td>
<td>View of data and operation of the WinCC project via the web</td>
<td>X</td>
</tr>
</tbody>
</table>
3.3.3 Engineering software components

SIMATIC WinCC is a modular system. Its basic components are the Configuration Software (CS) and Runtime Software (RT). Both software components are included in the full WinCC package (RC). The selection of the full package depends on the number of power tags (external tags) required to interface with the automation level.

The Configuration Software (CS) contains all the basic functions for engineering SIMATIC WinCC. The central component is the WinCC editor in which editors can be opened for configuring the various functions. Some functions that are recommended for a GMP environment are pointed out below.

Tag Management

In conjunction with SIMATIC S7, the variables (tags) can be managed centrally in the SIMATIC Manager and imported into the Tag Management of SIMATIC WinCC. This ensures consistency within the project.

Configuration Tool

The Configuration Tool provides the option of configuring mass data with the Microsoft Excel standard software. The Configuration Tool allows you to configure data from the tag management, alarm logging, tag logging and the text library. Data from existing projects, for example, can be used again. The WinCC configuration can be output as an overview and used for qualification.

SIMATIC Version Trail

SIMATIC Version Trail is a software option for versioning libraries, projects and multiprojects that can be used universally in the context of Totally Integrated Automation with SIMATIC.

With SIMATIC Version Trail, project data in the form of libraries, individual projects or complete multiprojects can be archived at a selected time. At the same time, SIMATIC Version Trail also handles the entire management of the version history. This means, for example, that once a version has been completed, it can no longer be modified.

SIMATIC Logon is needed for SIMATIC Version Trail.

WinCC/Audit Project Versioning

The WinCC/Audit RC and WinCC/Change Control options include the Project Versioning functionality. This allows versions of complete WinCC projects to be easily created in the form of one zip file. Data from linked WinCC Premium Add-ons, such as PM-QUALITY, are also included. The manually issued version ID is included in the name of the version created. An overview shows all versions along with the time stamps that have been produced for a WinCC project. If necessary, older project statuses can be recovered.

Change control with WinCC/ChangeControl

WinCC projects can be monitored for subsequent configuration changes by WinCC/Audit RC or by WinCC/ChangeControl. This, for example, provides infor-
mation on configuration changes that were carried out after acceptance of the project version.

A distinction is made between changes:

- that are transferred to the WinCC database, for example adaptations to tag management, in Alarm Logging, in Tag Logging etc.

- and changes that are carried out to WinCC configuration files, for example in process pictures, reports, scripts or even customer documents. These changes are recorded by the document control and involve the following documents:
  
  - Graphics screens (.PDL)
  - C & VBS project functions (.FCT, .BMO)
  - C & VBS global actions (.PAS, .BAC)
  - Report layouts (.RPL)
  - User documents (all valid user documents in the project folder Misc.Documents)
  - Graphics runtime settings (Gracs.ini)

If one individual document needs to be changed, it must be checked out, changed and then checked back in via document management. In the Audit trail, the file check out and check in is recorded with the time stamp, WinCC project name, file name, user ID and the entered comment. When checking in, the document control assigns documents write protection to protect them from changes.

**Note**

When changes are made to documents, document control makes it possible to recognize that a document has been changed; details of the change are, however, not recorded and should be described in comments.

It is important that the write protection of the files cannot be changed manually in Windows Explorer.

The various versions of the documents can be displayed in a history view.

**3.3.4 HMI level software components**

The runtime software (RT) is used to control and monitor the production process. The following sections discuss the functions for recording and displaying runtime data.
Alarm Logging

The entire message system is configured in Alarm Logging. This includes preparation, display, acknowledgment and archiving of process and system messages. Operator input in process pictures (for example changing an I/O value or clicking a button) also triggers an operator input message that is entered in Alarm Logging with its time stamp, user ID, old value, and new value.

Note

The Alarm Hiding functionality can be used to prevent selected messages from being displayed, for example during startup. Despite this, the messages are recorded in the WinCC Alarm Logging. More information on this can be found in the WinCC Information System.

Use of this functionality is the responsibility of the system operator and should therefore be coordinated with him.

Tag Logging

Archiving of process values is configured in the Tag Logging editor. Selected process values are recorded in definable acquisition cycles and stored in process value or compressed archives.

Managing data records with WinCC/User Archives

With the WinCC/User Archives option, recipe data or machine data records can, for example, be saved in the form of database tables.

To obtain an overview of the created data records in an archive, the ActiveX control WinCC/User Archives – Table Element is inserted in a WinCC picture with read access.

Automatic versioning of the data records is not supported with the WinCC/User Archives option. Versioning can be implemented during configuration. The user archives can be exported manually in CSV format.

Note

Operator input that causes changes to the database tables of WinCC/User Archives are recorded by WinCC/Audit.

See also

- WinCC Information System "Options > User Archives"

Audit Trail with WinCC/Audit

For production plants operated in a GMP environment, in 21 CFR Part 11, the FDA specifies the recording of changes to electronically managed records relevant for GMP including the time stamp, user ID, old value and new value in the form of an Audit trail. The WinCC/Audit option was developed for this functionality in SIMATIC WinCC. The option represents the various requirements that arise from the system architecture of WinCC as client/server system, as multiproject, etc., in terms of the Audit Trail. WinCC/Audit allows the user to implement one central Audit Trail over several server/client systems and several WinCC projects. WinCC/Audit not only
records the operator responses during runtime, but also changes in the engineering phase.

### WinCC/Audit

WinCC/Audit is made up of the following software packages:

- **WinCC/Audit RC** for configuration of the audit trail for operator actions during runtime and for engineering changes and recording the audit trail during operations

- **WinCC/ChangeControl RC** is for configuration of the audit trail for changes during configuration, that have been carried out, for example, on an approved product version

- **WinCC/Audit RT** is for recording the audit trail per station (server or client needed)

The following operations are recorded during runtime:

- All kinds of operator input during ongoing operation, such as login/logout, changes to I/O fields, dragging slider objects, selections in check boxes and text lists, etc.

- All changes in the user archives

- Operator input in external programs

The audit trail can be visualized with an Audit Viewer. A large number of standard and customized filters can be set in the Audit Viewer to specifically select or display the corresponding audit trail information. The audit trail information can also be exported or even printed out. The Audit Viewer is included in the scope of supply for the product.
For access control, WinCC/Audit works in conjunction with SIMATIC Logon software.

3.3.5 Long-term archiving

Long-term archiving of process values and messages can be set up using a long-term archive server or using the WinCC/CAS (Central Archive Server) option. Both concepts are introduced below.

WinCC long-term archive server

Both in WinCC Tag Logging and in WinCC Alarm Logging, there are options for long-term archiving. Apart from the archive size and segment change, the configuration for transfer to another computer can also be set.

The WinCC/DataMonitor option is used to view the data.

WinCC/CAS (Central Archive Server)

The process values and messages of up to 11 WinCC servers can be saved on one Central Archive Server (WinCC/CAS). The data is transferred to the CAS using the relevant configuration. Transparent access to the archived data is handled by the system automatically in the background. Only archive tags that are labeled as being of long-term relevance in WinCC Tag Logging are archived.

If the CAS computer is unobtainable, the completed archives remain on the WinCC servers and are transferred later on when the link to the CAS is reactivated.

Defined interfaces provide direct access to archived process values and messages. This means that important production data is available throughout the company.

Batch-oriented long-term archiving

For the batch-oriented recording of product-relevant data such as process values and messages, the WinCC Premium Add-on PM-QUALITY can be used (see chapter 3.4.3 “Batch-based long-term archiving with PM-QUALITY”).

3.3.6 Reporting

Report Designer

The SIMATIC WinCC Report Designer is used both for documentation of the WinCC configuration and for logging the runtime data.

Ready-to-use print jobs and report layouts are provided with SIMATIC WinCC. The preconfigured report layouts can be opened with the page layout editor of the Report Designer and modified as necessary.

The output options, scope and layout of these print jobs can also be modified. It is also possible to create application-specific print jobs.
Batch-based reporting

For the batch-oriented reporting of the recorded data, the WinCC Premium Add-on PM-QUALITY can be used, see chapter 3.4.2 "Batch-oriented reporting with PM-QUALITY".

3.3.7 Availability and plant configuration

Availability with WinCC/Redundancy

Availability can be increased by using

- redundant servers
- redundant communications paths
- fault-tolerant controllers

Two networked WinCC servers can be run in parallel to increase availability. Redundancy is configured using the WinCC/Redundancy option. Each WinCC server has its own process driver connection and has its own databases. During operation, both servers function in parallel and independently of one another and are available to the operator. Process values and messages are sent to each redundant server and processed there. Internal tags, internal messages (for example message acknowledgement) and user archives are synchronized directly online.

Once a failed server is returned to operation, an automatic archive update is run in the background. Any gaps that have occurred in the tag, message and user archives are filled and internal tags calibrated.
WinCC/DowntimeMonitor

The WinCC/DowntimeMonitor option is used to detect and analyze downtimes. Downtimes in machine- or production line-oriented manufacturing plants can be recorded centrally and analyzed. For individual devices, machines or entire production lines, specific characteristics can be recognized based on this information:

- OEE (Overall Equipment Efficiency),
- MTBF (Mean Time Between Failures),
- MRT (Mean Repair Time) and other Key Performance Indicators (KPI).

The following advantages result:

- Complete transparency for all machines as basis for optimizing the plant's productivity, in other words:
  - Avoiding disturbances and bottlenecks
  - Increasing availability
- Identification of specific characteristics (KPI)
- Integration of appropriate display instruments (controls) in WinCC process screens
- Can be used for individual machines or even complete production plants
- Distribution of evaluations to various people over the web

3.3.8 Interfaces to process data

WinCC/Web Navigator

The WinCC/Web Navigator option is used to set up remote access to the WinCC project. To view the process pictures, users with the necessary rights must authenticate themselves using their password. The details are checked by SIMATIC Logon. Working with process pictures is subject to the access protection defined in the User Administrator in the WinCC project.

WinCC/DataMonitor

WinCC/DataMonitor is a pure display and evaluation system for process data from WinCC, data from the WinCC long-term archive server or data from the WinCC Central Archive Server (CAS). WinCC/DataMonitor provides a number of analysis tools for interactive data display and for analysis of current process values and historical data:

- Excel workbooks
- Published reports
- Trends and alarms
- Process Screens
Web center

WinCC/Connectivity Pack
The WinCC/Connectivity Pack provides interfaces for access to archive data and messages in WinCC. WinCC provides access to the following process data:

- Alarms and Events (messages), OPC A&E, read and write (acknowledgments only) access
- Process value archives (trends), OPC HDA, read-only access
- Process tags (states), OPC DA, read and write access, ships with WinCC system software
- All archive data, WinCC OLE DB, read-only access

The WinCC/Connectivity Pack provides standardized access with OPC and OLE DB from computer systems at the plant and enterprise management levels to computer systems at the process level.

3.4 SIMATIC Additional Software
This manual introduces the following WinCC Premium Add-ons:

<table>
<thead>
<tr>
<th>Name</th>
<th>Brief Description</th>
<th>Additional license necessary</th>
</tr>
</thead>
<tbody>
<tr>
<td>PM-CONTROL</td>
<td>Recipe data management and order planning</td>
<td>X</td>
</tr>
<tr>
<td>PM-QUALITY</td>
<td>Batch-oriented recording of data and reporting</td>
<td>X</td>
</tr>
</tbody>
</table>

3.4.1 Batch-oriented control with PM-CONTROL
The WinCC Premium Add-on PM-CONTROL is a batch-oriented parameter control for recipe/product data management. The integrated order control allows flexible handling of production orders in which the recipe, production location, scalable production quantity and the time of production can be specified.

The software package is divided into three applications:

- Topology manager for mapping the process cell topology, creating the required parameters and configuring the interface to the automation level
- Recipe system for creating and managing recipes / products
- Order planning and order control, assignment and management of production orders

To achieve a cost-effective solution for both simple and more complex tasks, PM-CONTROL is available in the "Compact", "Standard" and "Professional" variants.
The use of SIMATIC Logon as central user administration can be set in PM-CONTROL.

3.4.2 Batch-oriented reporting with PM-QUALITY

The data recorded in the WinCC Premium Add-on PM-QUALITY can be displayed in trends (process values), printed as reports on a printer or exported as an HTML file, XML file or in database format. It is also possible to configure the export of batch data for long-term archiving on a different computer. (see chapter 6.6.2 "Batch-based long-term archiving with PM-QUALITY")

The software package includes the following applications:

- Topology Manager for mapping the plant topology and specifying the production data to be acquired
- Report Editor for creating the report layout for the acquired data and displaying batch reports on the screen
- Data Logging, runtime component for acquiring data
- Data View / Export View and various ActiveX Controls for displaying batch data
- Data Center, for merging the batch data (only in the redundant version)

Apart from the automatic acquisition of the configured batch data, manually entered values, for example laboratory values can be added to a batch report later. If the batch log is transferred to the archive automatically due to the set export option, no more changes can be made to the log if the "Complete automatically" option is set.

It is also possible to use a script in WinCC to configure an electronic signature of the batch logs by the logged-on user and with it the manual assignment of the batch status (released / locked).
3.4.3 **Batch-based long-term archiving with PM-QUALITY**

PM-QUALITY is a software package for batch-oriented acquisition of production data such as process values and messages.

The process values can either be taken from WinCC Tag Logging or recorded in a separate tag logging function, grouped according to the various acquisition cycles. Event-driven process values or those dependent on a trigger (for example set-points/actual values) are read in as snapshots. Alarm events and Audit Trail entries are taken from WinCC Alarm Logging.

Automatic export of the batch data can be configured in database format, in HTML format and/or in XML format. The PM-QUALITY application Export View (PM-QUALITY Client) can be used to view the batch data exported in database format.
4 System Installation and Configuration

The WinCC system software is available as a complete package (engineering and runtime software) or as a pure runtime package. The software is licensed using license keys graduated according to the number of power tags (external tags) for interfacing to the automation level.

In a multi-user system with server/client structure, the system software with the required number of power tags and the server option is installed on the WinCC server. With a basic configuration, the smallest RT license is adequate for clients.

4.1 Installation of the Operating System

Note
The computer name must comply with the WinCC naming convention before the MS SQL server is installed. The computer name cannot be changed later on. This requires the MS SQL server and WinCC system to be fully reinstalled.

See also
- WinCC Information System "Release Notes" and "Installation Notes"

4.2 SIMATIC Installations

4.2.1 SIMATIC WinCC

Note
WinCC is basically approved for operation in a domain or work group. Domain-group policies and domain restrictions can hinder the installation. In this case, remove the computer from the domain prior to installation. After the installation, the computer can be returned to the domain if the group policies and restrictions do not prevent operation of the WinCC software.

See also
- WinCC Information System "Release Notes" and "Installation Notes"
4.2.2 SIMATIC Security Control

SIMATIC Security Control is started automatically at the end of the WinCC installation and displays a dialog with the proposed settings. The settings are either made directly in the operating system using the **Accept** button or are saved using the **Save** button and made by a suitably authorized person later.

**Note**
The proposed settings must be accepted in order for the SIMATIC WinCC system software to function properly.

If the computer is part of another workgroup or domain, the application has to be run again.

SIMATIC Security Control is started again automatically if further settings are needed in the Windows operating system once WinCC options have been installed, for example the WinCC/Web Navigator option.

The settings are documented in XML format.

4.2.3 SIMATIC WinCC options

Further WinCC options and WinCC Premium Add-ons are installed only after the WinCC software has been installed.

4.2.4 Setting up long-term archiving

A separate computer should be set up in the network for the WinCC long-term archive server. The backup configuration of Alarm Logging and Tag Logging is configured so that the archive files are saved on this computer. (see also chapter \[3.3.5 Long-term archiving\])

The optional Central Archive Server (CAS) is also installed on a separate computer on which no other programs should be used.

**Note**
The paths defined when installing the CAS cannot be changed at a later date.

4.3 Setting up User Administration

One major requirement in a pharmaceuticals environment (21 CFR Part 11 and Annex 11 of the EU-GMP Guide) is system access protection. This includes setting up user groups. SIMATIC Logon allows graduation of operator input to the process within the SIMATIC WinCC system and certain options and Premium Add-ons.

The WinCC SIMATIC Logon option is based on Windows user management. SIMATIC WinCC and the WinCC Premium Add-ons work with SIMATIC Logon to provide access protection.
Note
The structure of the access protection should be decided before starting configuration.
All the permissions for working with the visualization user interface (faceplates, input boxes, buttons etc.) must be set up according to the specifications.

Note
Access security of the monitoring mechanisms must be configured in Windows (see chapter 4.3.2). The operating system user should not have administrator privileges. This ensures that only WinCC has access to the database. This means that access by the operating system to the SQL database is impossible.

The following sequence is recommended when setting up user administration:

- Setup of access protection in Windows (setting up of user groups and users)
- Installation and setup of the WinCC SIMATIC Logon option
- Setup of the access protection in **SIMATIC WinCC > User Administrator**

The individual applications can then be configured in any order:

- Assignment of permissions in the visualization user interface (picture window, input boxes, buttons)
- Setup of access protection for the WinCC/Audit option
- Setup of access protection in PM-CONTROL or PM-QUALITY if the WinCC Premium Add-ons are used
4.3.1 User administration on the operating system level

Since the user management of SIMATIC Logon is based on the mechanisms of the Windows operating system, there are always two options available for user management in Windows, either in a domain or in a workgroup with a central logon server.

Windows domain

With a domain server in the working environment, the advantages of the group and user management can be used in conjunction with SIMATIC Logon. The one-time administration of groups and users on the domain server enables all computers that belong to the domain to access the groups and users.

Note

When using multiple domain servers or when there are redundant servers, the domain structure ensures that users will still be able to perform operations and/or log on even if one domain server fails.

Windows workgroup

Within a work group, local users with identical tasks should be added to a local group. This group can then be granted the necessary authorizations.

If a computer is a member of a Windows workgroup, it must be specified which computer is the server in the workgroup. All user data are created and managed on this server. The data are made available from here to the other computers in the system.

SIMATIC WinCC supports the Windows permissions model. When SIMATIC WinCC is installed, the following local groups are set up:

- SIMATIC HMI
- SIMATIC HMI CS
- SIMATIC HMI VIEWER

SIMATIC WinCC manages the security settings and share rights automatically. To create and start a WinCC project, a user requires the administrator or power user status and, among other things, must be a member of the SIMATIC HMI group. The access rights within the WinCC project are checked by User Administrator.

See also

- SIMATIC WinCC Installation Notes
- SIMATIC HMI, Process Visualization System WinCC V6, Security Concept WinCC, chapter 4 "User and Access Management in WinCC and Integration in Windows Management"
4.3.2 Security settings in Windows

The users and groups are configured according to the specification in the user administration of Windows. With the Windows logon assigned to the various tasks, this achieves complete separation of computer access permissions, e.g., Windows users, from plant authorizations (plant operators).

The following local security settings are made in Windows:

- Password policies such as complexity, password length, password aging
- Account Lockout Policies
- Audit Policies

Note

After installing Windows, default parameters are set for the password policy, account lockout policy and audit policy. These settings must be checked and modified according to the applicable project requirements.

See also

- Operating system help of MS Windows or the appropriate Windows manual (for setting up Windows workgroups and the domain)
- WinCC Information System "Working with WinCC" (to set up user administration)
- SIMATIC HMI, Process Visualization System WinCC V6, Security Concept WinCC, chapter 4 "User and Access Management in WinCC and Integration in Windows Management"

4.3.3 Configuration of SIMATIC Logon

The possible and the necessary settings in the configuration of SIMATIC Logon described in the SIMATIC Logon configuration manual.

These settings include, for example:

- The logon of a "default user" after a user logoff
- Logon server ("working environment")
- Automatic logoff on using SIMATIC Logon
4.4 Administration of User Rights

The assignment of Windows groups to WinCC user groups is based on names. For example, the "Operator" Windows group will be assigned to a group of the same name "Operator" set up in the WinCC User Administrator. The Operator group is assigned the rights necessary for operator control in the WinCC system. The following procedure must be followed for this:

- Open WinCC project
- Open User Administrator using WinCC Explorer
- Create group(s)
- Assign permissions for each group

The check box for SIMATIC Logon must be selected in the User Administrator of the WinCC project.
See also

- WinCC Information System "Working with WinCC > Setting up User Administration"

### 4.5 Configuring Access Protection

#### Startup characteristics

Automatic startup and logon is described in chapter 5.1 "Startup Characteristics".

#### Disabling the Windows level during operation

Since access to the Windows operating system level should be avoided for security reasons, additional configuration settings are necessary. These settings avoid unauthorized access from the process mode of SIMATIC WinCC to sensitive data of the operating system.

**Note**

Access to the operating system level should only be permitted for administrators or maintenance personnel.

#### Configuration settings in WinCC

To prevent access to the operating system during process mode, all shortcut keys are disabled in the WinCC project in the "Computer properties" dialog.

Measures must be taken to ensure that ongoing operation can only be deactivated with appropriate operator permissions. After deactivation and a restart, the operating system can be accessed.

**See also**

- WinCC Information System "Installation Notes"

#### Preventing system access in object programming

Make sure that no objects are used in the user interface that permit access to the Windows file system or to executable programs. This risk exists, for example, with OLE objects, Internet links, online help system etc.
Configuration settings in Windows

The **Keep the taskbar on top of other windows** setting must be disabled in Windows.

In addition, attention must be paid that any HOT-KEY assignments are deactivated. HOT KEYs are normally used, for example, to influence the properties of the graphics card. By changing the graphics card properties, it is also possible to reach the operating system user interface.
5 Project Settings and Definitions

The SIMATIC WinCC system software allows very flexible configuration of customized process control and monitoring. A large part of the application software is configured here and extended functionality can be added with the aid of scripts.

Basic settings and procedures for configuring a WinCC project help to meet the GMP requirements and to limit the effort required for validating a system.

5.1 Startup Characteristics

Following the configuration phase, only the runtime component of WinCC is used for operator control and monitoring and for data archiving. To prevent unauthorized access to the system, the computer can be configured so that WinCC Runtime is activated automatically when the computer starts up.

Additional settings for the startup characteristics are made in the WinCC project. To do this, open the properties of the Computer object from the shortcut menu.
The WinCC components that were configured and must therefore be enabled during operation (for example Tag Logging, Alarm Logging etc.) are activated in the "Startup" tab.

5.2 Object-Oriented Configuration

By using faceplates, picture windows (for example for controlling process units such as valves, drives or similar) and user objects (for example for uniform visualization of objects) in WinCC, the configuration can be created object-oriented. The objects are first created for the various applications and tested with the customer before they are copied or instantiated in the configuration.

To create dynamic picture windows and user objects, a structure tag is preferred that bundles the various tag types for a process unit, for example a motor, in a self-defined data structure.

See also

- WinCC Information System
5.2.1 Faceplate types
A faceplate is a standardized picture object that is stored centrally as a type in a project. WinCC saves the faceplate type in an fpt file. This Faceplate type is inserted in a process picture as a faceplate instance.

On the one hand, these blocks can be stored in libraries but they are also simple to distribute and pass on since the entire information for a block is stored in a file. Subsequent changes to a faceplate type are automatically updated in all instances.

The faceplate properties are specified individually in a configuration dialog. To make objects dynamic, faceplate tags can be used. When they are instantiated, the faceplates are connected to the WinCC tag management.

5.2.2 User objects
A user object is an object whose graphic representation and dynamic characteristics are tailored to the requirements of the system. The object properties and the events that cause a dynamic response in the object are specified individually in a configuration dialog. Structure tags are recommend to make user objects dynamic.

User objects are either entered in the project library or collected together in a standard picture.

Reproducing a user object simply involves making copies of them. If any changes are made, the individual copies need to be updated manually.

5.2.3 Screen window
The picture window smart object allows a picture to be called within a picture. This functionality is used, for example, to call a window for controlling a process unit (valve, drive). Such an operator control picture is configured once for a particular function and then opened as an instance in a picture window. When the picture is called, a tag prefix is transferred.

5.2.4 Structure tag
Structure tags are used to make picture windows and user objects dynamic. A structure type is defined for a process unit, for example a motor, and contains all tag types for the motor as structure elements.
The example shows a simplified form.

5.2.5 Library of the Graphics Designer

The library contains numerous pre-configured graphic objects in the integrated **global library**. Graphic objects such as machines and plant components, measuring equipment, operator control elements and buildings are thematically organized. The library objects can be inserted in a screen with drag-and-drop and adapted as required.

To store user-defined objects, the **project library** can be used. User-defined objects that have been developed, tested and qualified individually are then available in the project library as a project standard for multiple use in process pictures.

**Note**
To keep the effort involved in qualifying process pictures to a minimum, it is advisable to use standard symbols whenever possible.

5.2.6 Project functions in the form of scripts

C and VB source files are programs written by the user that count as class 5 in the software categorization. This type of software is developed to meet customer-specific requirements that cannot be covered by the standard library.

If such functions are required more than once in the WinCC project, they should be configured in the Global Script editor as project functions. The function code is created once in the script, then tested and qualified. The function is then available throughout the entire project. The function call is simply programmed in the property for the picture object.

In general with such customized scripts, a greater effort for validation in the form of detailed functional and interface descriptions as well as documented tests should be included in the calculation.
5.3 Configuring Redundancy

The configuration dialog is opened using the Redundancy entry in WinCC Explorer.

Here, the settings for the connection to the redundant partner server are configured.

Selecting the Activate redundancy check box enables the data synchronization in redundant mode.

Synchronization of the internal tags must be configured separately for each tag. This is done by selecting the Tag synchronization check box in tag management in the properties dialog for tags.

Interaction with PM-QUALITY

The PM-QUALITY Professional with Data Center variant ensures that batch data is recorded in full in a redundant WinCC system.

Once a batch has been completed and released, the Data Center application merges the batch data recorded from two PM-QUALITY runtime databases into one export database. If one WinCC server is not available, the Data Center only becomes active when both WinCC servers are operating again.
Interaction with WinCC/Audit

In order to record the Audit Trail entries in a redundant system, the Audit Trail database can be stored on one of the redundant WinCC servers or set up on a computer in the network. If the WinCC server with the Audit Trail database fails, the records are buffered on the redundant partner server and added to the Audit Trail database once the down WinCC server is up and running again.

When configuring WinCC/Audit for a redundant system make sure that the This database receives audits from SEVERAL projects setting is selected when creating the database. This also has to be done if the database is stored locally on one of the redundant servers. This setting means that the partner server can access the WinCC/Audit database and buffering is handled correctly.

5.4 Clock Synchronization

In SIMATIC WinCC, the time transmitted on the bus as default is the standard world time UTC (Universal Time Coordinated).

To ensure that times match, all the stations belonging to the WinCC system must be synchronized to allow chronological processing (archiving trends, messages, redundancy synchronization of servers).

Time synchronization must also be activated on the engineering stations otherwise problems could arise when downloading changes.

Note
The activation of time synchronization is necessary in plants in which GMP is mandatory.
5.4.1 Concepts for time-of-day synchronization

The structure of the time-of-day synchronization must be carefully planned. Each time-of-day synchronization in the project is dependent on requirements. The requirements of time synchronization must be described in the function specification. The following sections introduce concepts in time synchronization.

Time synchronization in a Windows workgroup

The time in a workgroup should be synchronized via the WinCC server. The time of the WinCC server can also be synchronized using a time master such as SICLOCK.

Time-of-day synchronization in a Windows domain

If the automation system is operated in a Windows domain, the domain must serve as the time master. The time of the domain server can also be synchronized using a time master such as SICLOCK.

Note

The time on the clients in the domain is synchronized using Microsoft system services.

See also

- [http://www.siemens-edm.de/Siclock.zeitsynchronisationskonzept.0.html](http://www.siemens-edm.de/Siclock.zeitsynchronisationskonzept.0.html)
- WinCC Information System "Options > Options for Process Control > Time Synchronization"
- WinCC Information System "Release Notes > Process Control Options > Time Synchronization"
- SIMATIC HMI manual, Process Visualization System WinCC, Security Concept WinCC, chapter 5 "Planning Time Synchronization".

5.4.2 Time synchronization Central Archive Server (CAS)

The CAS must be linked to the project-dependent time synchronization concept. A time master, that supplies all other system components, including the CAS, with an actual time, must be declared in this time synchronization concept.
5.4.3 Time stamping

WinCC Alarm Logging

Messages archived from the automation system in WinCC Alarm Logging are given the time stamp either of the WinCC system or of the automation system SIMATIC S7-300/400.

With the bit message method, the message is detected due to a bit change in the message tag. Alarm Logging assigns the time stamp of the WinCC system. The time stamp has a certain inaccuracy due to the acquisition cycle, bus delay time and time required for processing the message. Messages present for a time shorter than the acquisition cycle are lost.

With the limit monitoring of tags in WinCC, a message is generated in Alarm Logging if the defined limit value is violated. The time stamp is set as in the bit message method.

Note
The bit message procedure and limit value monitoring can be used in a WinCC single user system. In redundant systems or WinCC systems with several operator stations, chronological signaling is used for coordinated acknowledgment and transmission.

For chronological signaling, the SFCs/SFBs Alarm, Alarm_S/SQ, Alarm_D/DQ, Alarm_8/8P are used on the SIMATIC S7. Refer to the relevant CPU manuals and the block descriptions in the SIMATIC STEP 7 online help for information on restrictions relating to the system resources for simultaneously pending alarms.

To use the chronological signaling function, the SIMATIC S7-400 in conjunction with the Alarm and Alarm 8/8P blocks is recommended.

See also

WinCC Tag Logging

Process values acquired and evaluated in WinCC Tag Logging are given the time stamp either with the time they are acquired in WinCC or with the value from the automation system.

To read in the process values cyclically, acquisition cycles are defined. The shortest acquisition cycle is 500 ms. A time stamp assigned when the process value is acquired includes the inaccuracy of the acquisition cycle.

Note
For acquisition cycles shorter than 500 ms, SFB37 (AR_SEND) is available on the SIMATIC S7-400.
Process values that receive their time stamp from the automation system are prepared in the form of a frame on the automation system and transferred as a raw data tag.

The specification (URS, FS) of a GMP-compliant plant must describe the way in which time stamping will be performed. The accuracy necessary for message and process value acquisition must be checked in detail. The methods of time stamping mentioned above can be used alongside each other.

5.5 Configuration Management

The configuration of a computerized system consists of various components both hardware and software; in a complex system these are often standard hardware and software components along with specially tailored user components. In the configuration management, the complete current system configuration must be available and clear to follow at all times. This is achieved by dividing the system into configuration elements, which can be identified by a unique designation and a version number and can be distinguished from the previous version.

Defining configuration elements

In the main standard components are used as the hardware, for example PCs, PLCs, monitors, panels, etc.

The standard components for software include, for example, the SIMATIC WinCC system software, its libraries, other options and Premium Add-ons.

The application software is configured and/or programmed on the basis of standard software. The individual configuration elements into which the application software should be split cannot be defined for all cases as it differs depending on different customer requirements and system characteristics.
Versioning the configuration elements

While the version ID of standard software cannot be changed by the user / configuration engineer, the issuing of version numbers and a procedure for change control must be defined in operating instructions etc. for configuring the application software. From when the application is first created, all configuration elements should be maintained following a defined procedure for configuration management even if it is only subject to formal change control at a later stage.

Note

Chapter 5.6 "Versioning Application Software" includes examples of how individual software elements can be versioned. Changes made to a plant in operation should always be agreed with the plant operator (see chapter 8.2 "Change Control during Operation").

See also

- GAMP5 Guide, Appendix M8 "Project Change and Configuration Management"

5.6 Versioning Application Software

The project guidelines must define which elements are to be versioned, when versioning is to take place, and whether a major version or minor version is to be incremented; for example:

"The major version is set to 1.0 following the FAT and to 2.0 after commissioning. All other changes are incremented in the minor version".

Whether the major version or the minor version is to be changed can also depend on the scope or effect of the change in question.

The following data is specified for the versioning of the application software:

- Name
- Date
- Version number
- Comment on the change

The following sections show various examples of software element versioning.
5.6.1 Versioning pictures in Graphics Designer

When the Graphics Designer editor is selected in WinCC Explorer, all existing process pictures are listed in the right window. The properties of every process picture can be displayed using the shortcut menu. The data shown is generated automatically by the WinCC system.

Additional information on versioning, for example the version ID, date changed and name can be entered in a static text box. It is practical to place the text boxes for versioning in a separate picture level that can be shown or hidden as required. The display of the static text box during process mode is controlled by the Display object property.
Project Settings and Definitions

Note
Details of a change can, for example, be described in the relevant validation documents.

Note
WinCC/Audit RC or WinCC/ChangeControl feature a document check with automatic versioning for WinCC pictures.

5.6.2 Versioning VB / C scripts
VB or C scripts are created to access tags and graphic picture objects during operation and to trigger actions that are not dependent on pictures.

Scripts are also used to link functions triggered during process mode to individual object properties in Graphics Designer (for example input using the mouse).

Two different methods of script creation are distinguished in WinCC:

- Picture-dependent VB / C scripts that are linked to the property of an object in the Graphics Designer WinCC editor. These scripts are part of the picture and are stored with the picture. Versioning is performed in the picture.

- Non picture-dependent VB / C scripts created in the Global Script WinCC editor.

VB / C scripts created with the Global Script editor provide boxes in the Properties dialog for entering the data Created By, Changed By, Version and Comment. The creation date and date of change are entered automatically by the WinCC system.

An optional password can also be assigned.
Note
If a password is used, this is not checked against the logged-on user. Knowing the password allows the script to be opened / edited. If the password is forgotten, access to the script is permanently denied.

It is advisable to maintain a history in the scripts indicating any changes made. The history is entered as comment before the start of the code. As an alternative, the comment box of the Properties dialog (see above) can also be used to record the history.

Example of recording the history in a C script:

```c
###
// Function: MyFunction
//
// History
// 05/01/2006  V1.0  Hans Meier  first version
// 05/03/2006  V1.1  Hans Meier  clear fault xxx
// 05/02/2009  V1.2  Paul Smith  add function yyy
#

void MyFunction()
{
    ...
}
```

Example of recording the history in a VB script:

```vb
Function MyProcedure
    History:
    01.05.2006  Hans Meier  first version
    03.05.2006  Hans Meier  clear fault xxx
    05.02.2009  Paul Smith  add function yyy

Sub MyProcedure
    End Sub
```

Note
WinCC/Audit RC or WinCC/ChangeControl feature a document check with automatic versioning for C / VB scripts.
5.6.3 Versioning reports

The automatic issuing of version IDs in the report layouts is not supported. A static field can be inserted in the report layout for a version ID allowing manual versioning of different states. The version ID must be kept up-to-date as specified in the SOP for configuration management. The following picture shows an example of a report layout footer with a field added for versioning.

![Versioning report layout](image)

**Note**
WinCC/Audit RC or WinCC/ChangeControl feature a document check with automatic versioning for report layouts.
6 Creating Application Software

In a full automation solution, SIMATIC WinCC handles the operator input, monitoring and data archiving functions. The interface to the automation level is powerful process links.

Chapter 6 explains the configuration of SIMATIC WinCC in a GMP environment based on examples. The configuration of the automation level is not described in this manual.

6.1 Creating the Graphic User Interface

To visualize the plant or process, process pictures are created to allow operator control and monitoring according to specified requirements. Their elements are described in chapter 5.2 "Object-Oriented Configuration".

In more complex processes, there will be several such process pictures for which it is advisable to define a system for picture selection and/or picture navigation. For the implementation, SIMATIC WinCC provides the Basic Process Control module.

The OS Project Editor is used to configure the WinCC project for standardized operator control of the process. Among other things, the monitor layout, monitor resolution, operating philosophy for the buttons, and message presentation are configured.

Both the overview graphics and the operator control philosophy must be described in the specification (for example URS, FS and P&I) and created accordingly. When completed, these should be shown in the form of screenshots to the customer for approval.

Note

The OS Project Editor should be configured before starting to create the process pictures because the size of the individual process pictures depends on the monitor resolution and screen layout.

6.2 Creating Operator Input Messages

For plants operated in a GMP environment, FDA regulation 21 CFR Part 11 requires that operator input to the process that affects data relevant to GMP can be traced.

GMP-relevant process input made using input/output boxes or buttons must therefore be configured in the WinCC Graphics Designer so that an operator input message is generated. This operator input message is recorded in WinCC Alarm Logging with the time stamp, user ID, old value and new value.
Input/output field

To create an operator input message for an I/O field object, the Operator input message property must be set to yes. If the Operator Activities Report property is also configured with yes, the system opens a window for entering comments after the value has been applied. The operator input permissions are also set in the object properties for the I/O box using the "Authorization".

Operator input messages in conjunction with faceplate tags

To generate operator input messages, the faceplate tag must not be attached directly to an I/O field as a dynamic variable but rather operator input message "yes" must be set in the properties. In this case, the value of the faceplate tags is set externally, for example by creating an I/O field outside the faceplate instance that is linked directly to a WinCC tag. This value is adopted in the output value of the faceplate tags. The properties and events of the faceplate variable must be suitably configured in advance.

Button

As default in WinCC, an operator input message is generated when a direct connection to a tag is configured. If the Operator Input Message check box is selected, the system generates a message. It is, however, not possible to enter an operator input comment here.
Script functions for value changes

If the options described for creating an operator input message for I/O boxes and buttons are not adequate, an operator input message can be generated using VB or C scripts. An example for a project function in C script can be downloaded at http://support.automation.siemens.com/DE/view/en/24325381.

Note
If the standard operator input message or the message numbers 1900000 to 1900050 are used when creating the operator input message, this is also automatically adopted by WinCC/Audit.

6.3 Electronic Signature

Operator actions in WinCC, for example, input via I/O fields or buttons, can be configured so that an electronic signature is requested from the user.

Example: The Start / Stop buttons turn the air-conditioning on or off. When the button is clicked, a picture window opens in which the user signs electronically by confirming his user ID and password. The button function is executed only after a successful signature. In the background a script containing the SIMATIC Logon VB function VerifyUser is executed. This function authenticates the logged-on user using the password entered. This electronic signature is demonstrated by an audit trail entry. (see chapter 6.4 “Audit Trail”)
During operation the details of the electronic signature have the following appearance:

### User operating

<table>
<thead>
<tr>
<th>Air condition</th>
<th>Temperature</th>
<th>Humidity</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2.0°C</td>
<td>0.0%</td>
</tr>
</tbody>
</table>

### Elektronik signature

- The Air condition will be switched on
- Benutzer-ID: engin
- Name: Meier Hans
- Password: 

To record an Audit Trail of user actions involving data relevant for GMP, WinCC provides several options: Alarm Logging from WinCC and the WinCC/Audit option. Both variants are introduced below.

#### 6.4 Audit Trail

To record an Audit Trail of user actions involving data relevant for GMP, WinCC provides several options: Alarm Logging from WinCC and the WinCC/Audit option. Both variants are introduced below.

#### 6.4.1 Audit trail via WinCC Alarm Logging

Operator input through input/output fields or buttons can be configured in the Graphics Designer in WinCC so that and operator input message is generated by the system. (for configuration, see chapter 6.2 "Creating Operator Input Messages")

To display login and logout activities in the WinCC system, the display of system messages is generally set up in WinCC Alarm Logging.
The operator input message is a system message for which the system automatically enters the old value in process value 2 and the new value in process value 3. We therefore recommend that you rename process value blocks 2 and 3.

For displaying operator input messages, use of the AlarmControl called WinCC Alarm Control (Classic) is recommended. In a process picture, the WinCC Alarm Control (Classic) is then dragged from the object palette to a picture in the Graphics Designer.
Double-clicking on the control opens the Properties dialog. To ensure that only operator input messages are displayed, a selection must be made. The Selection button opens the configuration dialog. Under System Blocks > Message Classes, the System message, without acknowledgement is selected. On the right in the detailed window, the operator input message must simply be selected.
To allow entries for the login / logout of a user to be shown in the Audit Trail, the type must be changed from process control to operator input message by double-clicking in the "Type" column for the message numbers 1008000 to 1008007 in WinCC Alarm Logging. For Web applications, the message numbers 1012400 and 1012401 must also be changed as described above.

The display of the message blocks is configured in the "Message Lists" tab.

The Audit Trail is displayed in the process picture as follows:

The symbol in the Comment column shows that a comment exists. This can be displayed with the button marked in the screenshot.
6.4.2 Audit trail via WinCC/Audit

Configuring the Audit Trail of operator input

The runtime monitoring components are enabled in the configuration dialog of the WinCC/Audit option. Runtime Data / Archives monitors entries both in the message / process value archives and in the user archives. Enabling Operator Actions records operator input during operation in the Audit Trail. The logon/logoff procedures during operation are also saved in the Audit Trail.

The recording of the operator control elements in the Audit Trail is enabled for each individual object in each process picture. The display of user comments can also be enabled.

The InsertAuditEntry function is also used to create Audit Trail entries. This function can be linked both in C and VB scripts. This allows user-specific audit trail entries to be generated, for example due to events or changes in object properties.

Setting up SIMATIC Logon for the WinCC/Audit option

If the SIMATIC Logon software is used, this needs to be set in the WinCC/Audit configuration editor using the Tools > Options menu.

The operating permissions in WinCC/Audit are governed via the Audit Admin and AuditDocControl user groups. The help system for WinCC/Audit provides detailed information.

Displaying, printing and exporting the Audit Trail via Audit Viewer

The Audit Viewer displays the content of the selected WinCC Audit Trail. The Audit Viewer is installed as a separate program. Numerous different filters can be set to filter out information important to the application. WinCC/Audit provides custom filters that display commonly required queries directly.

To allow it to be used for other purposes, the generated audit trail can be exported in the formats PDF, CSV, Microsoft Excel or XML (with checksum) and it can also be output to a printer.

To view the audit trail in plant pictures during WinCC runtime, the Audit Viewer application can also be linked into a WinCC picture as an OCX.
Backup configuration for Audit Trails in WinCC/Audit

To back up the Audit Trail database, the ArchiveAuditDB function is available as a runtime function. A precise description of this function can be found in the Audit help.

As an alternative, the MS SQL Server Management Studio or during runtime "Management > Maintenance Plans" can be used.

6.5 Recording and Archiving Data Electronically

It is very important to provide full quality verification relating to quality-relevant production data, especially for production plants operating in a GMP environment.

There are several steps involved in electronic recording and archiving:

- Definition of the data to be archived, the archive sizes and the suitable archiving strategy
- Setup of process value archives for the online storage of selected process values
- Setup of parameters for transferring the archives to the archive server (time period or amount of storage space occupied)

6.5.1 Specifying the data to be archived

Various factors must be taken into account when defining the archiving strategy and determining the required storage space, for example:

- Definition of data of different origins that need to be archived (process values, messages, batch data, reports, audit trails, log files etc.).
- Definition of the relevant recording cycles
- Specification of the periods of storage online and offline
- Definition of the archiving cycle for transfer to external storage

These data are stored in various archives:

- "Tag Logging Fast" process value archive
- "Tag Logging Slow" process value archive
- Alarm log
- WinCC reports

On top of this, in other parts of the system, actions are monitored and recorded in log files or databases:
- Change log on STEP 7 level for "Downloading the Target System" and online parameter changes
- SIMATIC Logon Eventlog
- Event Viewer under Windows Computer Management (logon/logoff activities, account management, rights settings for the file system, etc. according to the corresponding configuration)

All the files mentioned (and others, if required) must be considered in the archiving concept.

6.5.2 Setting up user archives

Creating database tables with several data sets in the User Archives editor supports the adherence to GMP requirements in terms of the audit trail of parameter data (recipe data / machine data).

This is done by creating I/O fields in a WinCC picture and linking them with the relevant data fields. With suitable configuration, the input of a value triggers an operator input message.

When using the WinCC/Audit option, the parameter data records can be entered directly in the User Archive ActiveX table. There is no need to divert the data input via I/O fields to create an operator input message. Entries in the table are transferred directly into the WinCC/Audit database.

See also
- WinCC Information System

6.5.3 Recording and archiving

Archiving in WinCC involves two steps. First, messages and process values are recorded in WinCC Alarm Logging (message archive) or WinCC Tag Logging (process value archive).
These short-term archives can be backed up in a long-term archive using a number of different solutions and can then be stored for a period specified by the customer.

Data recording in SIMATIC WinCC

To archive alarms and process values in a GMP environment, the setting **Signing activated** must be selected in the relevant configuration dialog ("Alarm Logging", "Tag Logging Fast" and "Tag Logging Slow"). When the data is transferred, an internal algorithm generates a checksum. This means that subsequent manipulation is detected by the system and is displayed when a connection is established to a manipulated database.

To prevent losses due to failure of the long-term archive, an alternative second target path can be specified.
Long-term archiving with SIMATIC Central Archive Server

The Central Archive Server (CAS) that can be implemented redundantly as an option is a dedicated server without a direct process connection. The archived data of all the servers in the system (message archives, process value archives and reports) can be transferred to the CAS and archived there.

Compared with WinCC long-term archiving, archived data can be retained in the CAS for a much longer time due to the greater capacity.

Batch-based long-term archiving with PM-QUALITY

In PM-QUALITY, the acquired batch data can be exported in database, HTML or XML format manually or automatically. Collecting and recording these data is described in chapter 6.6.2 "Batch-oriented reporting with PM-QUALITY".

Only completed batches can be archived. Selecting the Automatic batch finalize check box in the Project Settings > Defaults dialog has the effect that changes to the batch data are no longer possible after the automatic export.

For export in HTML format or XML format, subsequent manipulation of the data can be prevented by assigning the appropriate rights to the drive (read-only) or by subsequent automatic converting into PDF format with the help of further tools.

See also

- Online help for the PM-QUALITY product

6.6 Reporting

6.6.1 Reporting with WinCC Report Designer

The Report Designer is integrated in the WinCC system software to allow documentation of the configuration data and the runtime data.
The following runtime data can be logged:

<table>
<thead>
<tr>
<th>Runtime Data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message sequence log</td>
<td>Chronological listing of all messages that have occurred</td>
</tr>
<tr>
<td>Alarm report</td>
<td>Messages of the current message list</td>
</tr>
<tr>
<td>Archive report</td>
<td>Messages from the message archive, for example based on operator input messages</td>
</tr>
<tr>
<td>Audit trail</td>
<td>With the option Audit logged operator actions</td>
</tr>
<tr>
<td>Tag table</td>
<td>Tag contents from process value / compressed archives in the form of a table</td>
</tr>
<tr>
<td>Tag trend / picture</td>
<td>Tag contents from process value / compressed archives in the form of a trend</td>
</tr>
</tbody>
</table>

The contents of user archives can also be documented in the form of a table.

**Note**

WinCC Report Designer supports reporting of continuous processes.

A series of system layouts and system print jobs for various documentation requirements are supplied with the product.

The layouts can be used to create new layouts or print jobs but they should not be modified. Changing the system layout means additional test effort from a GMP perspective. If the system software is upgraded, the system layouts are overwritten by the installation.

**See also**

- The WinCC Information System "Working with WinCC > Documentation of Configuration and Runtime Data > Appendix > System Layouts and Print Jobs for Runtime Documentation"

**Page layout editor**

The page layout editor of the Report Designer is used to modify system layouts to meet users' needs or to create new layouts. System layouts are opened in the page layout editor and saved under a new name so that they can be modified.

**Print jobs**

The Audit Trail entries are shown in the log as follows:

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>User name</th>
<th>Tag</th>
<th>Old value</th>
<th>New value</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>30.11.2008</td>
<td>11:31:00</td>
<td>Hans Meier</td>
<td>Setpoint1</td>
<td>5</td>
<td>6</td>
<td>X</td>
</tr>
<tr>
<td>30.11.2008</td>
<td>11:31:00</td>
<td>Hans Meier</td>
<td>Setpoint2</td>
<td>4</td>
<td>5</td>
<td>X</td>
</tr>
<tr>
<td>30.11.2008</td>
<td>11:31:00</td>
<td>Hans Meier</td>
<td>Setpoint1</td>
<td>8</td>
<td>8</td>
<td>X</td>
</tr>
</tbody>
</table>

**See also**

- WinCC Information System "Working with WinCC > Documentation of Configuration and Runtime Data"
Creating Application Software

**Reporting Audit Trail entries from WinCC/Audit**

The Audit Trail entries from the WinCC/Audit database can be printed using the Report Designer. To do this, a new data source must be created for the SQL server.

![Create a New Data Source to SQL Server](image)

The default database is set to **WinCC_Audit**.

**6.6.2 Batch-oriented reporting with PM-QUALITY**

The WinCC Premium Add-on PM-QUALITY is used for batch-oriented archiving and reporting. The recording of the production-relevant data begins with the **Batch start** signal and ends with the **Batch end** signal. The data is assigned to a specific batch, which can be configured, and called back up again with the batch name.

The report layouts for printing the batch data can be customized in the Report Editor application.

The procedure for including Audit Trail entries (operator input messages) in a batch log is shown below based on an example.

The alarm blocks to be shown in the batch report are selected in the properties of the **Audit Trail alarm group**. The message number for the operator input message as defined in the WinCC system is also entered in the message filter dialog.

The **Audit Trail alarm group** is displayed in the area for the existing objects in the Report Layout editor. The Audit Trail alarm group is dragged to the right to be included in a report layout.
An Audit Trail can appear as follows in a batch report:

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>User name</th>
<th>Old value</th>
<th>New value</th>
<th>Comment-Text</th>
<th>Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/26/2003 2:35:20 PM</td>
<td>Hans Meyer</td>
<td>0.000000</td>
<td>1.000000</td>
<td></td>
<td>MX_BatchActive</td>
</tr>
<tr>
<td>9/26/2003 2:35:43 PM</td>
<td>Hans Meyer</td>
<td>5.000000</td>
<td>6.700000</td>
<td>Value to small Setpoint_1</td>
<td></td>
</tr>
</tbody>
</table>

Change comments can be logged in the audit trail.

See also
- Online help for WinCC Premium Add-on PM-QUALITY

6.7 Monitoring the System

6.7.1 Diagnostics of communication connections

WinCC provides the Channel Diagnosis application for monitoring communication connections to the lower-level controllers. The application can be integrated in a WinCC picture (for example a diagnostics picture) via Start > SIMATIC > WinCC > Tools > Channel Diagnosis or as an ActiveX Control. The status of the channels that support diagnostics is displayed in a window. Information on the start / end of the connection, version ID and error messages with time stamp are automatically recorded in a log file. This represents evidence of the quality of the communication connections provided by the system.
### 6.7.2 System information channel

The system information channel is used to evaluate system information such as drive capacity, CPU load, server monitoring by a client, date, time and much more. The system information channel is configured as a separate connection. The relevant system function is linked to a system tag for display / evaluation.

In a GMP environment, it is often necessary to archive large amounts of data. By configuring the system information channel, the capacity of the hard disk can be monitored. If a definable limit value is exceeded, a reaction can be configured, for example a message in Alarm Logging.

The display of the relevant system tag could, for example, be configured in a diagnostics picture along with the ActiveX control *Channel Diagnosis*.

### 6.7.3 Lifebeat monitoring

The Lifebeat Monitor monitors all servers, clients and automation devices which can be reached over PC networks and industrial networks (Industrial Ethernet, PROFIBUS or OPC).

To configure the nodes to be monitored, the *Lifebeat Monitoring* editor is opened in WinCC Explorer. Here, all the nodes to be monitored and the monitoring cycle in which the lifebeat monitoring takes place can be set up.
6.8 Data Exchange with the Plant Management Level

Date communication with the plant management level or other systems must be covered by system functionalities. Here, there are several options available, including the integrated OPC connection (OPC Data Access), the connections of OPC A&E and OPC Historical Data Access, or the WinCC OLE DB connection.

Data exchange with WinCC/Connectivity Pack

The WinCC/Connectivity Pack option makes standardized access to the WinCC data possible. This option is installed on the WinCC server.

The following mechanisms are available:

- OPC Historical Data Access (HDA)
- OPC Alarms and Events (A&E)
- WinCC OLE DB

Data exchange with Connectivity Station

The Connectivity Station software package offers the same functionality as the aforementioned Connectivity Pack. The difference is in the installation. The Connectivity Station can be installed on any PC in the network.

Data exchange with IndustrialDataBridge

The IndustrialDataBridge application offers various mechanisms for the exchange of data between WinCC and various applications, for example an Oracle database. Archived data cannot be manipulated.

Data exchange via the ODK programming interface

The WinCC Open Development Kit (ODK) option describes the exposed programming interfaces that can be used to access data and functions of the WinCC configuration and WinCC runtime system.

6.9 Connecting to a Web Client

When talking about web access from a computer in the network to a WinCC project, a distinction is made between read-only access and read and write/user input access. While the WinCC/Web Navigator option can be used to set up read-only as well as write access, the WinCC/DataMonitor can be used as an alternative for read-only access. Operator input via the web client is checked by both the SIMATIC logon (user authentication) and the user administrator in WinCC (operator permissions).

See also

6.9.1 Setting up operator permissions on the WinCC server

The operator permissions in the web client are set up in the WinCC User Administrator. The User Administrator editor is opened in WinCC Explorer for this purpose.

Checking the check box for SIMATIC Logon activates authentication of the user logged on via SIMATIC Logon. (see also chapter 4.3.3 "Configuration of SIMATIC Logon")

Remote access is activated by selecting the check box for the Web Navigator.

The "DataMonitor – Monitor only" function controls operator permissions between Web Navigator and DataMonitor. If this function is not activated and the Web Navigator license is detected, the operator can control the process pictures. If this function is activated, the process pictures can only be monitored.
Note
This configuration is undertaken separately for each user group. This means that the definitions for release for remote access, the start page, language and operator permissions may be different for each user group.

6.9.2 Remote access via the network

The web client must be installed on the computer for remote access.

The WebViewer is installed automatically when the WebClient is installed. For remote access, it is advisable to use this in preference to the Internet Explorer since the WebViewer can be configured individually.

For initial parameter assignment and further usage, WinCCViewerRT.exe is called in the path in which the WebClient was installed, for example: C:/Programs/Siemens/WinCC/Web Navigator/Client/Bin. The first time this is called, parameters are assigned to the WebViewer:

See also
- WinCC Information System "WinCC/Web Navigator Documentation > Use of the Terminal Services for WinCC/Web Navigator > WinCCViewerRT"

The time configured here for the automatic logout is relevant for the logout characteristics of the remote access. When using the WebViewer, specifying the logout time when configuring the WebViewer is adequate (see above). According to the settings configured here, the WebClient prompts for confirmation of the logout in the Web one minute before the specified time:
The settings are stored as default in the "WinCCViewerRT.xml" configuration file. When the dialog is exited with the "OK" button, the connection to the Web server is established. The configured parameter settings are set for future WebViewer sessions. The next time the WebViewer is started, the parameter assignment dialog is not opened. If parameter settings need to be modified later, the XML file must be deleted. The configuration dialog is then displayed again when the WebViewer is started.

Logons and logoffs via the Web are logged in WinCC Alarm Logging:

To be able to see the logons and logoffs via the Web in the report, the operator input messages must be changed from process control to operator input messages. (See chapter 6.4.1 "Audit trail via WinCC Alarm Logging")

6.9.3 Web access to display data

Apart from the WinCC/Web Navigator, the Trends & Alarms application of the WinCC/DataMonitor option is used to display and evaluate the archived data either from WinCC or from the long-term archive server. Trends & Alarms and the other tools available grant read-only access to the archived data.

The process screens with the WinCC Alarm Logging and/or Tag Logging controls can be used as an alternative for viewing data.

Using Internet Explorer, the archive data can be displayed on any computer in the network.

The Archive Connector tool is used to connect/disconnect the archived database with/from the MS SQL server.
6.10 Interfaces to SIMATIC WinCC

6.10.1 Interfacing SIMATIC WinCC flexible

SIMATIC WinCC can also be used as a SCADA system (Supervisory Control and Data Acquisition) to which one or more lower-level systems are connected.

See also
- GMP Engineering Manual SIMATIC WinCC flexible, Siemens AG, I IA VMM Pharma

6.10.2 Interfacing SIMATIC S7

Connection via defined channels

To exchange data between WinCC and the automation systems, the first thing that is required is a physical communications connection that is configured in SIMATIC WinCC.

A connection is configured for the selected channel unit in the tag management by creating the tags with a name and data type. These tags are also known as external tags.

The tag management forms the data interface between the automation system and WinCC system. All the editors integrated in WinCC read / write data to the tag management.

An interruption to the communication connection is indicated in the WinCC Alarm Logging if system messages are enabled.

Evaluating the tag status and quality status

To allow monitoring, a status value and a quality code are generated for each tag. Among other things, the tag status indicates configured limit value violations and the link status between WinCC and the automation level. The quality code is a statement about the quality of the value transfer and value processing.

The evaluation of the tag status or the quality code can be configured, for example in the dynamic values dialog in the properties of a graphic object.
The checking of the quality code and tag status can also be performed in VB / C
scripts and linked to a user-defined action.

See also

- GMP Engineering Manual SIMATIC STEP7,
  Siemens AG, I IA VMM Pharma

6.10.3 Interfacing third-party components

Connection via defined channels

We recommend that the OPC channel is used as the communication connection
between WinCC and third-party automation devices. The communication driver for
OPC (OLE for Process Control) is certified by the OPC Foundation. The driver is
included in the WinCC system software.

It is possible to link the OPC client with third-party control systems over an OPC
server.

In tag management (data manager), a communication connection is configured for
the OPC channel in which tags with name and type can be created.

WinCC also operates as an OPC DA server and transfers process values to other
OPC clients.
7 Support During Qualification

The following graphic shows an example of a lifecycle approach. After creation of the system, the system must be tested to establish whether all specified requirements are met. GAMP5 calls this phase the "Verification". The terms "validation" and "qualification" are not replaced by this but rather supplemented. The areas covered by tests performed by the supplier and suitably documented can be used for the validation activities of the pharmaceuticals company.

Various standard functionalities of SIMATIC WinCC can be used as support in verification/qualification.

7.1 Qualification Planning

In defining a project life cycle, various test phases are specified. Therefore, basic qualification activities are defined at a very early stage of the project and fleshed out in detail during the subsequent specification phases.

The following details are defined at the outset of the project:

- Parties responsible for planning and performing tests and approving their results
- Scope of tests in relation to the individual test phases
- Test environment (test structure, simulation)
Support During Qualification

Note
The work involved in testing should reflect not only the results of the risk analysis, but also the complexity of the component to be tested. A suitable test environment and time, as well as appropriate test documentation, can help to ensure that only very few tests need to be repeated, or even none at all.

The individual tests are planned in detail at the same time as the system specifications (FS, DS) are compiled. The following are defined:

- Procedures for the individual tests
- Test methods, e.g. structural (code review) or functional (black box test)

7.2 Qualification of the Hardware

During the qualification phase, tests are performed to verify whether the installed components and the overall system design meet the requirements of the Design Specification. This includes details such as component name, firmware / product version, installation location, server and clients used, interfaces to the automation systems, etc.

Aids in the qualification of the system hardware

- Printouts and screenshots as proof in the qualification
- Additional visual checks of the hardware when necessary
- Printouts of the hardware configuration; as well as checking that it matches the switching cabinet documentation
- Printout of the SIMATIC NetPro configuration
- PC pass with information on all installed hardware and software components. This can be created manually or using commercially available tools. Where necessary, there should also be an additional visual check

7.3 Qualification of the Software

Aids in the qualification of the system software

Files, printouts and screenshots of various functions and programs can be used as proof for the qualification, for example:

- Installed software, chapter 7.3.2
- Report Designer, chapter 6.6.1
- SIMATIC Security Control, chapter 7.3.2
- Diagnostics of communication connections, chapter 6.7.1
- System information channel, chapter 6.7.2
7.3.1 Software categorization according to GAMP Guide

According to the GAMP Guide, the software components of a system are assigned to one of four software categories for the purpose of validating automated systems.

In terms of a WinCC system, this means that the individual software components require different degrees of effort for specification and testing depending on their software category.

While a computer system as a whole would usually have to be assigned to category 4 or sometimes even 5, the individual standard components to be installed (without configuration) involve effort analogous to category 3 or 1.

The configuration part based on installed products, libraries, function blocks etc. then corresponds to category 4.

If “free code” is then programmed as well, this corresponds to category 5 and involves significantly more effort for specification and testing.

7.3.2 Qualification of standard software

During qualification of the standard software used, checks are made to verify whether or not the installed software meets the requirements of the specifications. This includes:

- Operating system and other software packages
- SIMATIC WinCC system software
- SIMATIC standard options (Audit, DataMonitor, User Archives, etc.)
- SIMATIC WinCC Premium Add-ons (PM-CONTROL, PM-QUALITY)
- Standard libraries

The software installed on the operating system can be checked with Control Panel > Add/Remove Programs.

The settings required in the Windows operating system for the WinCC system software can be queried in the SIMATIC Security Control application: Start > Programs > SIMATIC > Security Control > Accepted settings. (see also chapter 4.2.2 “SIMATIC Security Control”)
Detailed documentation of the installed SIMATIC software can be found under Programs > SIMATIC > Product notes > Installed software.

The **Automation License Manager** program provides information on the installed licenses on the WinCC computer.
7.3.3 Qualification of the application software

During the verification/qualification of the application software, test descriptions are generated according to the stipulations of the software specification and the application software is tested on the basis of these.

The following checks are typical when testing a computer system:

- Name of the application software
- Technological hierarchy (plant, plant section, technical equipment, individual control element etc.)
- Software module test (typical test)
- Communication to other nodes (controllers, MES systems etc.)
- Inputs and outputs
- Control module (device control level)
- Equipment phases and equipment operations
- Relationships between modes (MANUAL/AUTOMATIC switchovers, interlocks, start, running, stopped, aborting, completed etc.)
- Process tag designations
- Visualization structure (P&I representation)
- Operating philosophy (access control, group rights, user rights)
- Archiving concepts (short-term archives, long-term archives)
- Signal concept
- Trends
- Clock synchronization

Configuration data such as the tags, functions or graphics used can be output based on reports. There are preconfigured standard layouts and print jobs for this that can be edited with the aid of the Report Designer. (See chapter 6.6.1 "Reporting with WinCC Report Designer")

7.4 Configuration Control

7.4.1 Project versioning

Versioning with "SIMATIC Version Trail"

Within the framework of Totally Integrated Automation (TIA), the WinCC HMI system is integrated in the SIMATIC Manager. The WinCC project has been integrated in the STEP 7 project. In this case, the SIMATIC Version Trail option is recommended for versioning. SIMATIC Version Trail supports the archiving of projects...
and assignment of a version ID (name and version number). A major version and minor version can be distinguished and a comment can be entered.

SIMATIC Version Trail manages all actions relating to a project, such as creating, archiving, and deleting versions in the version history.

When using SIMATIC Version Trail for continuous archiving, the version history provides a good way of documenting various software statuses during the life cycle of a computerized system.

All software versions are listed in chronological order, together with their archiving date and version.

See also

- GMP Engineering Manual SIMATIC STEP7, Siemens AG, I IA VMM Pharma
Versioning with "WinCC/Audit Project Versioning"

When not in integrated mode, we would recommend the WinCC/Audit Project Versioning option for versioning WinCC projects. This application can be used to manage several WinCC projects. The WinCC project must be closed for versioning.

A table-based list shows the versions created for the WinCC project selected on the left in the tree structure. A new archive is created or an older project version retrieved using the buttons positioned at the top.

Manual project versioning

In this storage concept, it might be specified, for example, that the project is backed up following a change. The project can be backed up with the WinCC tool Project Duplicator that creates a copy of the WinCC project in the specified path. The WinCC project must be closed before it is copied.

As an alternative, the folder containing the WinCC project is compressed in Windows Explorer to back up a project.

A version ID can, for example, be included in the file name of the compressed file. When compressing the WinCC project, it is important that the folder hierarchy is retained so that the project can be read again later.

Versioning data in WinCC options / add-ons

If options or Premium Add-ons such as PM-CONTROL / PM-QUALITY are used in the WinCC project, the corresponding databases must also be backed up. Before the data is backed up, a check must be made to ensure that the databases of the add-ons were disconnected from the MS SQL Server when the WinCC project was closed. Data of the WinCC options and add-ons stored in the default path under the WinCC project are also backed up by the Project Duplicator, by Version Trail and WinCC/Audit Project Versioning. If a user-defined storage path was specified during installation, the data must be backed up separately.
7.4.2 Change control of the configuration data

WinCC/Audit or WinCC/ChangeControl

Configuration changes in the WinCC project can be recorded using the WinCC/ChangeControl option. When tracking, a distinction is made between changes in the WinCC database and in the documents. The tracking of changes in both areas can be activated separately.

WinCC Explorer activation includes tracking changes in the following areas:

- WinCC Explorer
- Project properties
- Tag Management – apart from System parameters
- Alarm Logging
- Tag Logging – the most relevant changes to timers, archives and tag tables.
- Text Library – for entries in German, English, French, Italian, Spanish.
- User Administrator
- Report Designer print jobs
- User Archives
- Other editor programs whose configuration data are saved in the project’s CS database.
The screenshot shows two new tags that were created in WinCC tag management (EventType Insert). One of the tags was then renamed (EventType Update).

The *Document Control* area covers changes in the following areas:

- C project functions (.fct), global and local C-actions (.pas)
- VBS project functions (.bmo), global and local VBS actions
- Report layouts (.rpl)
- Graphics documents (.pdl)
- Server properties on the "Graphics Runtime" tab (gracs.ini)
- Client properties on the "Graphics Runtime" tab (gracs.ini)
- All user documents in the project folder *Misc. Documents*

Checked documents are write-protected and must be checked out before changes are possible. When checking in and checking out, entry of the comment is mandatory; the changes can be tracked based on this comment. The document's history records all the users who have checked the document in and out.
7.5 Backing Up the Operating System and SIMATIC WinCC

The operating system and the WinCC installation should be backed up as hard disk images. These images allow you to restore the original state of PCs without significant effort.

**Note**

An image can only be imported on a PC with identical hardware. For this reason, the hardware configuration of the PC must be adequately documented.

Images of individual partitions can only be exchanged between image-compatible PCs because various settings, for example in the registry, generally differ from PC to PC.
8 Operation, Service and Maintenance

8.1 Operation and Monitoring

SIMATIC WinCC provides extensive process visualization. Individually configured user interfaces can be configured for each application – for reliable process control and optimization of the entire production sequence.

Production can be monitored, controlled and optimized with plant intelligence and versatile interfaces. The central components in monitoring during operation are screen signals in graphics and faceplates along with trends, messages, acoustic signals etc.

Runtime data can be output by the system based on reports. There are preconfigured standard layouts and print jobs for this that can be edited with the aid of the Report Designer. (See chapter 6.6.1 “Reporting with WinCC Report Designer”)

The available data includes messages in chronological order, messages from a specific message archive, messages from the current message list, values from a process value and compression archive and data from applications not belonging to WinCC.

8.2 Change Control during Operation

Changes to validated and operational plants must always be planned in consultation with the plant user, documented and only made and tested after approval.

The following sections use examples to describe how to make changes to a WinCC project:

1. Initiation and approval of change specification by plant user

2. Description of the software change

3. Back up of the current WinCC project

4. Implementation of the software change including documentation based on the current version.

   WinCC/Audit is used to record changes in the engineering and in the document control in an audit trail. The versions of the project software and documents are also managed.

5. Test of changes incl. documentation

6. Backup of the changed WinCC project incl. versioning
The effects of the change to other parts of a WinCC application and the resulting tests must be specified based on risk and documented.

8.3 System Recovery

The procedure described in this section should enable the end user to restore the WinCC system after a disaster.

Disasters are taken to mean the following cases:

- Damage to the operating system or installed programs
- Damage to the system configuration data or configuration data
- Loss or damage to runtime data

The system is restored using the saved data. The backed up data (medium) and all the materials needed for the restoration (basic system, loading software, documentation) must be saved at the defined point. There must be a Disaster Recovery Plan which must be checked on a regular basis.

**Restoring the operating system and installed software**

The operating system and installed software are restored by loading the corresponding images (see chapter 7.5 "Backing Up the Operating System and SIMATIC WinCC"). The instructions provided by the relevant software supplier for the data backup application should be followed.

**Restoring the application software**

The process for restoring the application software depends on the kind of backup.

- Reading back the data using the software version trail
- Reading back the data using the software WinCC/Audit Project Versioning
- Reading back the data from a manually created backup
- Downloading the server data from the engineering station to the WinCC server using "Download to target system"

**Restoring the runtime data**

Runtime data, for example from Alarm Logging data and Tag Logging that has not been backed up using a backup configuration is lost in the event of a hard disk disaster.

To display lost data in WinCC Runtime, corresponding backup statuses with the extension mdf and ldf are copied back to the local computer and linked to the WinCC project using Connect archives.
When using a CAS, the data do not have to be copied back. The data are displayed directly in the OCX Alarm Control or Trend Control / Table Control by selecting the lost time period.

**Restoring a WinCC server in a redundant system**

After restoring the system, the WinCC project is started. The redundancy synchronization of the runtime databases is performed automatically.

**Restoring the long-term archive data on the CAS**

The best way to avoid data loss due to hard disk defects is to use RAID systems.

Regular checks of the operating system’s event log and a Raid controller with adequate performance are also required for this.

Restoring on a new hard disk by reinstalling is also possible if the configuration data is currently available.

Data not yet transferred to archive (at least the part which comes from the WinCC servers) is not lost because depending on how the times overlap it usually still exists on the WinCC servers as part of the short-term archive that has not been overwritten.
8.4 Uninterruptible Power Supply (UPS)

An uninterruptible power supply (UPS) is a system for battery backup of the supply voltage. If the power supply fails, the battery of the UPS takes over as the power supply. When power is restored, the UPS battery discontinues serving as the power supply and the battery is recharged. A few UPS systems offer not only battery backup of the power supply but also the possibility of supply voltage monitoring. They ensure an output voltage without interference voltages at all times.

Systems with higher priority are, for example:

- Automation system (AS)
- Network components
- Archiving server
- WinCC server
- WinCC clients

In each case it is important to include the systems for data reporting in the battery backup. The reporting should also include the time of the power failure.

The following should also be remembered:

- Configuration of alarms regarding power failure
- Determination of the time frame for shutting down the PC
- Specification of the time frame of the UPS battery backup
9 System Updates and Migration

9.1 Updates, Service Packs and Hotfixes

It is essential that system software updates for a validated, operational plant are agreed with the user. An update such as this represents a system change, which must be planned and executed in accordance with the applicable change procedure. Similar to the description in chapter 8.2 “Change Control during Operation”, this roughly means the following steps:

- Describe the planned change
- Effects on functions / plant units / documentation
  inclusion of the system description of the new and modified functions in the readme file/release notes
- Assess risks
- Define the tests which need to be performed to obtain validated status, based on the risk assessment
- Approve/reject the change (in accordance with defined responsibilities)
- Update of the technical documentation
- Execute the change in accordance with manufacturer documentation (as the plant has been released for it)
- Document the activities performed
- Qualification: Carry out and document the necessary tests

In considering possible influences, the following may be relevant:

- Process screens / objects / alarm system and process value logging in function and display
- Interfaces
- Effects during download
- System performance
- Documentation (specifications)
- Qualification tests to be repeated or performed for the first time

Note
Support for software updates and project migration is available from SIMATIC Product Support at http://support.automation.siemens.com
9.2 Migration of the Application Software

The WinCC system software is upgraded with a migration, in other words, its range of functions is expanded or improved.

When there is a version change (for example from version 5.x to version 6.x) or a software update of the WinCC system software, it may be necessary to migrate or convert data created with the older version.

See also

- WinCC Information System "Upgrading from WinCC > Notes on Migrating Projects"

The Project Migrator application is available for migration. The project data is migrated offline, the WinCC system software must be completely closed down. Follow the instructions of the Project Migrator. If adaptation of the project is necessary, this requires validation.

The validation effort is decided in consultation with the plant operator. Possible test points are the new functions available in WinCC and the correct installation of the software components required for migration.
Index List

A
Access management .......................... 11, 32, 37
Alarm Logging .............................. 23, 45
Application software ....................... 53
Archive per station .......................... 15
Archiving
Online ........................................... 22
Audit trail ...................................... 14, 23, 56
Alarm Logging .................................. 56
WinCC/Audit .................................. 60, 66
Audit Viewer .................................. 24
Availability .................................. 26

B
Backup ........................................... 83
Batch data .................................. 14
Batch-oriented control ...................... 28

C
Category
hardware ....................................... 10
software ....................................... 10
Central Archive Server (CAS) ............ 25
Long-term archiving ....................... 64
Time synchronization ....................... 45
Change control ................................ 84
Clock synchronization ...................... 16, 44
Configuration management ............... 10, 47
ConfigurationTool ......................... 21
Connectivity Station ....................... 69

D
Data backup .................................. 15
Data exchange .............................. 69
Diagnostics .................................. 67

E
Electronic records ......................... 12
Electronic signature ....................... 13, 55
Engineering software ..................... 21

F
Faceplate types ................................ 41

G
GMP requirements .......................... 10
Guidelines .................................. 7

H
Hardware category .......................... 10
Hotfix ........................................... 88

I
IndustrialDataBridge ....................... 69
Installation
Operating system .......................... 31
SIMATIC Security Control ............... 32
SIMATIC WinCC ............................ 31
SIMATIC WinCC options .................. 32
Interface
Process data .................................. 27
S7 .............................................. 73
Third-party component .................... 74
WinCC flexible ............................. 73

L
Life cycle model ............................ 7
Lifebeat Monitoring ....................... 68
Logging ....................................... 14, 25, 29, 64, 66
Readback ..................................... 15
Long-term archive server ............... 25
Long-term archiving ....................... 25, 30, 32, 64

M
Migration ..................................... 89
Monitoring .................................. 67

O
Object-oriented configuration .............. 40
Operator input message .................. 53
Ordinance .................................. 7
Overview diagrams ....................... 53

P
Page layout editor ......................... 65
Password .................................. 12
Print jobs .................................. 65
Process images ................................ 53
Project settings .......................... 39

Q
Qualification ................................ 75
Application software ..................... 75
Standard software ....................... 77
Qualification planning .................... 75
<table>
<thead>
<tr>
<th>Index List</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>R</strong></td>
</tr>
<tr>
<td>Redundancy ........................................... 43</td>
</tr>
<tr>
<td>Report Designer ........................................ 25, 64</td>
</tr>
<tr>
<td>Restore ................................................. 85</td>
</tr>
<tr>
<td><strong>S</strong></td>
</tr>
<tr>
<td>Safety ...................................................... 18</td>
</tr>
<tr>
<td>Screen window ........................................... 41</td>
</tr>
<tr>
<td>Script ..................................................... 42, 49</td>
</tr>
<tr>
<td>Service pack ............................................... 88</td>
</tr>
<tr>
<td>SIMATIC Logon ........................................... 20, 35</td>
</tr>
<tr>
<td>Software category ......................................... 10, 77</td>
</tr>
<tr>
<td>Specification .............................................. 19</td>
</tr>
<tr>
<td>Startup characteristics ................................... 39</td>
</tr>
<tr>
<td>Structure tag ............................................... 41</td>
</tr>
<tr>
<td>System installation ........................................ 31</td>
</tr>
<tr>
<td>System library ............................................. 42</td>
</tr>
<tr>
<td>System specification ....................................... 17</td>
</tr>
<tr>
<td><strong>T</strong></td>
</tr>
<tr>
<td>Tag logging ................................................ 23, 46</td>
</tr>
<tr>
<td>Third-party components .................................... 16</td>
</tr>
<tr>
<td>Time stamp ................................................... 45</td>
</tr>
<tr>
<td>Typical ...................................................... 11</td>
</tr>
<tr>
<td><strong>U</strong></td>
</tr>
<tr>
<td>Uninterruptible power supply (UPS) ....................... 86</td>
</tr>
<tr>
<td>User administration ......................................... 11, 20, 32</td>
</tr>
<tr>
<td>User archives .............................................. 62</td>
</tr>
<tr>
<td>User ID ...................................................... 12</td>
</tr>
<tr>
<td>User objects .................................................. 41</td>
</tr>
<tr>
<td>User rights .................................................. 36</td>
</tr>
<tr>
<td><strong>V</strong></td>
</tr>
<tr>
<td>Validation Manual .......................................... 8</td>
</tr>
<tr>
<td>Verification ................................................ 75</td>
</tr>
<tr>
<td>Version Trail ................................................ 21, 79</td>
</tr>
<tr>
<td>Versioning ................................................... 79</td>
</tr>
<tr>
<td>Application software ........................................ 47</td>
</tr>
<tr>
<td>Audit Project Versioning ................................... 21, 80</td>
</tr>
<tr>
<td>Configuration elements ..................................... 47</td>
</tr>
<tr>
<td>Pictures ..................................................... 48</td>
</tr>
<tr>
<td>Reports ....................................................... 51</td>
</tr>
<tr>
<td>Script ....................................................... 49</td>
</tr>
<tr>
<td>Visualization hardware .................................... 17</td>
</tr>
<tr>
<td><strong>W</strong></td>
</tr>
<tr>
<td>Web access</td>
</tr>
<tr>
<td>Data display ................................................ 72</td>
</tr>
<tr>
<td>Operator permissions ....................................... 70</td>
</tr>
<tr>
<td>Remote ....................................................... 71</td>
</tr>
<tr>
<td>Web Client ................................................... 69</td>
</tr>
<tr>
<td>WinCC add-on ................................................. 81</td>
</tr>
<tr>
<td>PM-CONTROL .................................................. 28</td>
</tr>
<tr>
<td>PM-QUALITY ................................................... 29, 30, 43, 64, 66</td>
</tr>
<tr>
<td>WinCC option ................................................ 81</td>
</tr>
<tr>
<td>Audit ......................................................... 21, 23, 24, 44, 81</td>
</tr>
<tr>
<td>CAS ........................................................... 25</td>
</tr>
<tr>
<td>ChangeControl ............................................... 21, 24, 81</td>
</tr>
<tr>
<td>Connectivity Pack .......................................... 28, 69</td>
</tr>
<tr>
<td>DataMonitor .................................................. 25, 27, 69</td>
</tr>
<tr>
<td>DowntimeMonitor ............................................ 27</td>
</tr>
<tr>
<td>Open Development Kit (ODK) .............................. 69</td>
</tr>
<tr>
<td>Redundancy ................................................... 26</td>
</tr>
<tr>
<td>User Archives ............................................... 23</td>
</tr>
<tr>
<td>Web Navigator ............................................... 27, 69</td>
</tr>
</tbody>
</table>
SIMATIC WinCC V7.0
Guidelines for Implementing Automation Projects in a GMP Environment

Siemens AG
Industry Sector
Industry Automation
VMM Pharma
76181 KARLSRUHE
GERMANY
pharma.aud@siemens.com
www.siemens.com/simatic-wincc