



SIEMENS

Edition

07/2024

GMP ENGINEERING MANUAL

SIMATIC

SIMATIC WinCC V8.0

Guidelines for Implementing Automation Projects in a GMP Environment
[siemens.com/pharma](https://www.siemens.com/pharma)

SIMATIC

SIMATIC WinCC V8.0 GMP Engineering Manual

Configuration Manual

Introduction

Configuring in a GMP
Environment

1

Requirements for
Computer Systems in a
GMP Environment

2

System Specification

3

System Installation and
Basic Configuration

4

Project Settings and
Definitions

5

Creating Application
Software

6

Support for Verification

7

Data Backup

8

Operation, Maintenance
and Servicing

9

System Updates and
Migration

10

Abbreviations

A

Guidelines for Implementing Automation Projects in a
GMP Environment

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.

DANGER

indicates that death or severe personal injury **will** result if proper precautions are not taken.

WARNING

indicates that death or severe personal injury **may** result if proper precautions are not taken.

CAUTION

indicates that minor personal injury can result if proper precautions are not taken.

NOTICE

indicates that property damage can result if proper precautions are not taken.

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, 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 complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens Aktiengesellschaft. 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 the manual

This manual contains instructions for system users and configuration engineers for integrating SIMATIC systems into the GMP environment (GMP = Good Manufacturing Practice). It covers validation and takes into account special requirements of international regulatory bodies and organizations, such as 21 CFR Part 11 of the FDA or EU GMP Guide Annex 11.

This manual describes what is required from the pharmaceutical, regulatory viewpoint (in short: GMP environment), of the computer system, the software and the procedure for configuring such a system. In the following chapters, practical examples are used to explain the relationship between requirements and implementation.

To suggest improvements to this document, please use the contact details provided at the back of this manual.

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.

Validity of the manual

The information described in this manual is valid for SIMATIC WinCC V8.0. The examined components are SIMATIC WinCC (Configuration and Runtime) in combination with the options WinCC/Audit, WinCC/WebNavigator, WinCC/DataMonitor and the WinCC Premium Add-ons PM-CONTROL, PM-QUALITY, PM-OPEN IMPORT, PM-ANALYZE and PM-LOGON. Refer to the product catalog or the compatibility tool for information on the compatibility of the individual components with SIMATIC WinCC.

- Product Catalog ST 80 (<https://support.industry.siemens.com/cs/ww/en/view/109744146>)
- Compatibility tool (<http://www.siemens.com/kompatool>)

Any questions about the compatibility of the SIMATIC WinCC Premium Add-on products should be addressed directly to the supplier, see here (<https://www.siemens.com/process-management>).

Position in the information landscape

The system documentation of the SIMATIC WinCC 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 PDF format.

This manual supplements the existing SIMATIC WinCC manuals. It is not only useful as a guideline during configuration, it also provides an overview of the requirements for configuration and what is expected of computer systems in a GMP environment.

Structure of this manual

The regulations and guidelines, recommendations and mandatory specifications are explained. These provide the basis for configuration of computer systems.

All the necessary functions and requirements for hardware and software components are also described; this 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 can be found in the standard documentation.

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 the central training center in D 90327 Nuremberg, Germany.

Internet (<http://www.sitrain.com>)

Siemens on the Internet

You can find a guide to the technical documentation available for the individual SIMATIC products and systems here at:

SIMATIC HMI technical documentation (<https://support.industry.siemens.com/cs/ww/en/view/109744536>)

The online catalog and online ordering system are available at: (<http://mall.industry.siemens.com/>)

You can find additional information about the products, systems, and services from Siemens for the pharmaceutical industry at: (<http://www.siemens.com/pharma>)

as well as information about the WinCC Premium Add-ons at: (<https://www.siemens.com/process-management>)

You can contact the WinCC Center of Competence in Mannheim by e-mail at WinCCAddon.automation@siemens.com

Technical support on the Internet

You can find comprehensive information about our Service and Support at: (<https://sieportal.siemens.com/en-ww/home>)

Industry Online Support offers there for example:

- Manuals and product information
- FAQs and application examples

You can also find on this page:

- Services in a comprehensive overview, e.g. information about on-site service, repairs, spare parts, and much more
- A bulletin board in which users and specialists worldwide exchange their know-how
- mySupport for personal filters, notifications, support requests, among other things, our newsletter containing up-to-date information on your products.

Additional support

If you have any further questions about the use of products described in this manual, and do not find the right answers there, please contact your local Siemens representative and offices.

Find your personal contact partner at: (<https://www.siemens.com/global/en/general/contact.html>)

If you have questions on the manual, please contact:

E-mail: pharma@siemens.com

Table of contents

	Introduction	3
1	Configuring in a GMP Environment	11
1.1	Regulations and guidelines	11
1.2	Lifecycle model	11
1.3	Responsibilities	12
1.4	Approval and change procedure	13
1.5	Risk-based approach.....	13
2	Requirements for Computer Systems in a GMP Environment	15
2.1	Categorization of hardware and software	15
2.2	Test effort depending on the categorization.....	15
2.3	Change and configuration management.....	16
2.4	Software creation	16
2.5	Access control and user administration.....	17
2.5.1	Applying access control to a system.....	17
2.5.2	Requirements for user IDs and passwords	17
2.6	Requirements for electronic records	18
2.7	Electronic signatures	18
2.8	Audit trail	19
2.9	Reporting batch data	19
2.10	Archiving data	20
2.11	Data backup	20
2.12	Retrieving archived data.....	21
2.13	Time synchronization.....	21
2.14	Using third-party components.....	21
3	System Specification.....	23
3.1	Selection and specification of the hardware.....	24
3.1.1	Hardware specification.....	24
3.1.2	Selecting the hardware components	24
3.2	Security of the plant network	25
3.3	Specification of the basic software.....	26
3.3.1	Operating system.....	27
3.3.2	Basic software for user administration	27
3.3.3	Software components for engineering	27
3.3.4	Software components for HMI level.....	28

3.3.5	Long-term archiving.....	30
3.3.6	Reporting	31
3.3.7	Availability and plant configuration	32
3.3.8	Interfaces to process data.....	33
3.4	Application software specification	34
3.5	Additional SIMATIC software	35
3.5.1	Batch-based control with PM-CONTROL	36
3.5.2	Batch-based reporting with PM-QUALITY	36
3.5.3	Batch-based long-term archiving with PM-QUALITY	37
3.5.4	Importing archives with PM-OPEN IMPORT	37
3.5.5	Evaluation and analysis of logs with PM-ANALYZE.....	37
3.6	Utilities and drivers	38
3.6.1	Printer drivers	38
3.6.2	Virus scanners	38
3.6.3	Image & partition tools	38
4	System Installation and Basic Configuration	39
4.1	Installation of the operating system	39
4.2	Installation of SIMATIC components	39
4.2.1	SIMATIC WinCC	40
4.2.2	SIMATIC Security Controller.....	41
4.2.3	SIMATIC WinCC options	42
4.2.4	Setting up long-term archiving	42
4.3	Setting up user administration	42
4.3.1	User administration on the operating system level.....	44
4.3.2	Security settings in Windows.....	45
4.3.3	SIMATIC user groups	46
4.3.4	Configuration of SIMATIC Logon	47
4.3.5	Logon via RFID card reader with PM-LOGON	49
4.3.6	Monitoring access protection	50
4.3.7	Administration of authorizations	50
4.3.8	Assigning authorizations	52
4.4	Access control to operating system level.....	52
4.4.1	Startup characteristics.....	53
4.4.2	Disabling the operating system level during operation	55
4.5	Data and information security	57
5	Project Settings and Definitions	63
5.1	Project setup.....	63
5.1.1	Creating a project	63
5.1.2	Multi-user engineering.....	63
5.2	Object-oriented configuration	64
5.2.1	Faceplate types	64
5.2.2	User objects.....	64
5.2.3	Picture window	65
5.2.4	Structure tag.....	65
5.2.5	Graphics Designer libraries	66
5.2.6	Project functions in the form of scripts	66

5.3	Configuring redundancy.....	67
5.4	Time synchronization.....	68
5.4.1	Time synchronization concepts	69
5.4.2	Time stamping.....	69
5.5	Configuration management	71
5.6	Versioning application software	71
5.6.1	Versioning pictures in Graphics Designer	72
5.6.2	Versioning VB / C scripts	73
5.6.3	Versioning reports	75
5.6.4	Versioning of the entire WinCC project	76
6	Creating Application Software	77
6.1	Creating the graphic user interface.....	77
6.1.1	Standardized user interface.....	78
6.1.2	Creating process pictures in the Graphics Designer	79
6.1.3	Password protection for process pictures	79
6.2	Creating operator input messages	80
6.3	Audit trail and change control	84
6.3.1	Audit trail for operator actions.....	84
6.3.2	Change control for the configuration and project engineering.....	87
6.4	Electronic signature	88
6.5	Recording and archiving data electronically	90
6.5.1	Determining the data to be archived.....	90
6.5.2	Setup of process value and message archives	91
6.5.3	Setting up user archives	92
6.5.4	Recording and archiving.....	92
6.5.5	Long-term archiving.....	93
6.6	Reporting	94
6.6.1	Reporting with the WinCC Report Designer.....	95
6.6.2	Batch-based reporting with PM-QUALITY	96
6.7	Monitoring the system.....	98
6.7.1	Evaluation of performance tags.....	98
6.7.2	Diagnostics of communication connections.....	99
6.7.3	Diagnostics for SIMATIC S7-1200 / S7-1500 channel	99
6.7.4	System information channel.....	100
6.7.5	Lifebeat Monitoring	101
6.8	Data exchange with the plant control level	101
6.9	Connecting via web	103
6.9.1	Setting up user authorizations on the WinCC server.....	104
6.9.2	Remote access via the network with the WebNavigator	105
6.9.3	Web access for data display	107
6.9.4	Web access for mobile devices.....	107
6.10	Interfaces to SIMATIC WinCC	108
6.10.1	Interfacing to SIMATIC WinCC.....	108
6.10.2	Connection to SIMATIC S7	109
6.10.3	WinCC Cloud Connector	111

6.10.4	Interfacing third-party components	111
7	Support for Verification	113
7.1	Test planning	113
7.2	Verification of the hardware	114
7.3	Verification of the software	115
7.3.1	Software categorization according to GAMP Guide	115
7.3.2	Verification of standard software	116
7.3.3	Verification of application software	118
7.4	Configuration control	119
7.4.1	Versioning	119
7.4.2	Change control	121
7.4.3	Write protection	121
8	Data Backup	123
8.1	Backup of the system installation	123
8.2	Data backup of the application software	124
9	Operation, Maintenance and Servicing	127
9.1	Operation and monitoring	127
9.1.1	Process visualization	127
9.1.2	Audit trail review	127
9.2	Operational change control	128
9.3	System restoration	128
9.4	Uninterruptible power supply	130
10	System Updates and Migration	131
10.1	General procedure	131
10.2	Updating the system software	132
10.3	Migration of the application software	132
10.4	Validation effort for migration	133
A	Abbreviations	135
	Index	137

Configuring in a GMP Environment

As a prerequisite for configuring computer systems in the 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

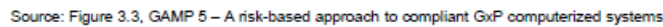
The regulations, guidelines and recommendations of various national and international authorities and organizations have to be taken into account when configuring computer systems requiring validation in the GMP environment. Regarding computer systems, the following are of particular significance:

Title (Author)	Subtitle	Area of application
21 CFR Part 11 (US Food and Drug Administration, FDA)	Electronic Records, Electronic Signatures	Law/regulation for manufacturers and importers of pharmaceutical products for the U.S. market
Annex 11 of the EU GMP Guide (European Commission)	Computerised systems	Binding directive within the European Union for implementation in relevant national legislation
GAMP 5 (ISPE)	A Risk-Based Approach to Compliant GxP Computerized Systems	Guideline with worldwide validity as recommendation

1.2 Lifecycle model

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

The following figure shows the general approach of GAMP 5 for the development of computerized systems. It begins with the planning phase of a project and ends with the start of pharmaceutical production following completion of the tests and reports.



Once production has started, the system lifecycle continues until decommissioning.

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

Responsibilities for the activities included in the individual lifecycle phases must be defined when configuring computer systems in a GMP environment and creating relevant specifications. As this definition is usually laid down specific to a customer and project, and requires a contractual agreement, it is recommended to integrate the definition in the Quality and Project Plan.

- GAMP 5 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 maintain validated status, which means ensuring the traceability of the steps undertaken.

Before setting up or modifying a system, it is therefore necessary to plan, document and obtain the customer's or plant operator's approval of the pending steps in terms of functionality and time.

1.5 Risk-based approach

Both the U.S. FDA ("Pharmaceutical cGMPs for the 21st Century Initiative", 2004) and the industry association ISPE/GAMP ("GAMP 5" Guide, 2008) recommend a risk-based approach to the validation of systems. This means that question as to whether or not to validate a system and the extent a system should be validated depends on its complexity and its influence on the product quality.

Requirements for Computer Systems in a GMP Environment

2

This chapter describes the essential requirements an automated system in the GMP environment must meet regarding the use of computerized systems. These requirements must be defined in the specification and implemented during configuration. In case of subsequent changes or interventions in the system, reliable evidence must be provided at all times, regarding who, at what time, and what was changed or implemented. The requirements for 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 these requirements with a specific system is dealt with starting from chapter "System Specification (Page 23)".

2.1 Categorization of hardware and software

Hardware categorization

According to the GAMP 5 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 5 Guide, the software components of a system are divided into various software categories. These range from commercially available and pre-configured "standard" software products that are merely installed, to configured software products and customized applications ("programmed software").

2.2 Test effort depending on the categorization

The effort involved in validation (specification and testing) is much greater when using configured and, in particular, customized products compared to 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 Change and configuration management

All the controlled elements of a system should be identified by name and version and any changes made to them should be checked. The transition from the project phase 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

- GAMP 5 Guide,
Appendix M8 "Project Change and Configuration Management"

2.4 Software creation

Certain guidelines must be followed during software creation and documented in the Quality and Project Plan (in the sense of the Good Engineering Practice, in short GEP concept). Guidelines for software creation can be found in the GAMP Guides as well as the relevant standards and recommendations.

Use of type/instance concepts and copy templates

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 potential supplier audit to be performed.

Therefore, to keep validation work to a minimum, preference should be given to standardized blocks during configuration (products, in-house standards, project standards). From these, customized types and templates are created and tested according to the design specifications.

Identification of software modules/types/copy templates

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

Changes to software modules/types/copy templates

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 control and user administration

To ensure the security of computer systems in the GMP environment, such systems must be equipped with an access control system. In addition to physical access control to certain areas, access-control systems protect computer systems against unauthorized logical access. Users are assembled into groups, which are then used to manage user permissions. Individual users can be granted access authorization in various ways:

- Combination of unique user ID and password; see also chapter "Requirements for user IDs and passwords" (Page 17)
- RFID / smart cards together with a password
- Evaluation of biometrics, e.g. fingerprint scanners

2.5.1 Applying access control to a system

In general, actions that can be performed on a computer system must be protected against unauthorized access. Depending on a user's particular field of activity, a user can be assigned various permissions. Access to user administration should only be given to the system owner or to a very limited number of employees. Furthermore, it is absolutely essential that unauthorized access to electronically recorded data is prevented.

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

Note

Access to PCs and to the computer system must only be possible for authorized persons. This can be supported by appropriate measures such as mechanical locks and through the use of hardware and software for remote access.

2.5.2 Requirements for 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:

For creation of passwords, a minimum number of characters and the expiry period of the password should be defined. In general, a password should comprise a combination of characters that meet the minimum length requirement as well as at least three of the criteria listed below.

- Use of uppercase letters
- Use of lowercase letters

2.7 Electronic signatures

- Use of numerals (0-9)
- Use of special characters

See also

- Chapter "Setting up user administration (Page 42)"

2.6 Requirements for electronic records

The following requirements additionally apply to the use of electronic records for relevant data:

- The system must be validated.
- Only authorized persons must be able to enter or change data (access control).
- Changes to data or deletions must be recorded (audit trail).
- Electronic records that are relevant for long-term archiving must be stored 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 batch production record is used, its structure and contents must match the structure and contents of the master production record. As an alternative, the master production record and batch production record can also be combined in one document.

See also

- EU GMP Guide, chapter 4.9 and Annex 11
- 21 CFR Part 11 "Electronic Records, Electronic Signatures", U.S. FDA

2.7 Electronic signatures

Electronic signatures are computer-generated information which acts as a legally binding equivalent to handwritten signatures.

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

Electronic signatures are relevant in practice, for example, for manual data inputs and operator interventions during runtime, approval of process actions and data reports, and changes to recipes.

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

Note

During the production of drugs and medical devices, which enter the U.S. market, the FDA regulations must be met. This is 21 CFR Part 11 with respect to electronic signatures.

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 in which a smart card replaces one of the two identification components.

These identifying components can, for example, consist of 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.

Biometric characteristics include fingerprints, iris structure, etc.

2.8 Audit trail

The audit trail is a control mechanism of the system that allows all data entered or modified by the operator to be traced back to the original data. A secure audit trail is particularly important when GMP-relevant electronic records are created, modified or deleted.

Such an audit trail must document all the changes made to GMP-relevant values "in normal operation" along with the date and time. The audit trail contains information on who changed what and when (old value / new value), as an option it may also include "why".

2.9 Reporting batch data

In the production of pharmaceuticals and medical devices, batch documentation takes on a special significance. For pharmaceutical manufacturers, methodically created batch documentation is often the only documented evidence within the framework of product liability.

2.11 Data backup

The components of batch documentation are as follows:

- Master production record and batch production record
- Packaging instructions and packaging record (from a pharmaceutical point of view, the packaging of the finished drug is part of the manufacturing process)
- Test instructions and test report (relating to all quality checks, for example in the chemical analysis)

The batch production record or packaging record has a central significance here and this is defined below:

- The batch production record is always both product-related and batch-related.
- It is always based on the relevant parts of the valid master production record.
- It contains all process-relevant measurement and control processes as actual values.
- It also contains deviations from the specified setpoints.

2.10 Archiving data

(Electronic) archiving means the permanent storage of electronic data and records in long-term storage.

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

Based on predicate rules (EU GMP Guide, 21 CFR Part 210/211, etc.), the customer must decide how electronic data is stored and, in particular, which data is affected by this. This decision should be based on a reasonable and documented risk assessment that takes into account the significance of the electronic records over the retention period.

If the archived data are migrated or converted, the integrity of the data must be assured over the entire conversion process.

See also

- GAMP 5 Guide, Appendix O13 "Archiving and retrieval"

2.11 Data backup

In contrast to the archiving of electronic data, data backups are used to create backup copies, which ensure system restoration if the original data are lost or a system failure occurs.

The backup procedure must include periodic backups of non-retentive information to avoid total loss of data due to system components failures 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.

Data backups are created on external data carriers. The data media 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).

See also

- GAMP 5 Guide, Appendix O9 "Backup and restore"

2.12 Retrieving archived data

It must be ensured that archived/backed up data can be read back at any time. If a system update/migration is to be performed, compatibility of the archived data before the update must be ensured. If required, the archived data must also be migrated.

See also

- GAMP 5 Guide, Appendix O13 "Archiving and retrieval"
- GAMP 5 Guide, Appendix D7 "Data migration"

2.13 Time 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, see also ISO 8601) is recommended as the time base for saving data. The time stamp of messages and values can be displayed in local time with a note indicating daylight saving time/standard time.

2.14 Using third-party components

When third-party components (hardware and software) are used, their compatibility to other components in use must be verified. If components specifically "tailored" (customized) to individual projects are used, a supplier audit should be considered in order to check the supplier and their quality management system.

See also

- GAMP 5 Guide, Appendix M2 "Supplier Assessment"

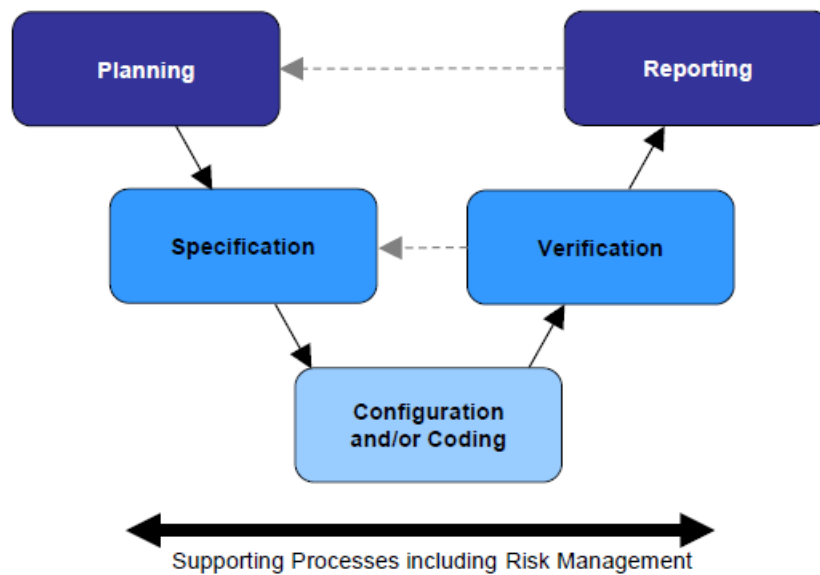
2.14 Using third-party components

System Specification

During the specification phase for a computer system, the system to be built and its functionality are defined in as much detail as is required for implementation.

Specifications not only represent the basis for a structured and traceable configuration but are – particularly in the GMP environment – an essential reference for final verification of the system.

The specification covers the selection of products, product variants, options, and system configurations, as well as the application software.



Source: Figure 3.3, GAMP 5 – A risk-based approach to compliant GxP computerized systems

It is possible to divide the full specification, for example, into:

- Functional specification (FS/FDS) as a response to user requirement specifications (URS)
- General configuration and design (system design, general topics)
- Hardware (and network) design specification (HDS)
- Software design specification (SDS)
- HMI specification

3.1 Selection and specification of the hardware

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

- Single-station system with complete operation control and monitoring of a production process on one single PC
- Multi-station 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 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 verification.

- Hardware overview diagram, system structure and organization
- Control cabinets (control cabinet names, UPS configuration, location), PC stations, control cabinets, automation system with CPUs, I/O cards, etc.
- PC components for server and client including their installation instructions
- Network structure for Industrial Ethernet, e.g., switches, names and IP addresses of PC stations, Ethernet configuration, general network settings
- Time synchronization for hardware
- Field devices

The HDS can be an integral part of an overall specification or be extracted into a separate document.

Note

The information in the hardware overview diagram and the naming of hardware components must be unequivocal.

See also

- GAMP 5 Guide, Appendix D3 "Configuration and Design"

3.1.2 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 can find details in the current product catalog.

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 together with a Panel PC as a complete HMI system.

System availability and data security, in particular for PC components with critical functions, can be increased by using a suitable class of RAID systems and with a redundant system design. In a redundant WinCC system hardware components such as WinCC server, screen and operator controls are set up twice. If one WinCC server fails, the other automatically takes over the functionality.

Note

We recommend using the approved hardware from the current product catalog (<https://support.industry.siemens.com/cs/ww/en/view/109744146>). These components have been checked for compatibility by Siemens in system tests. The use of unreleased configurations requires additional effort for specification and test phase.

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

3.2 Security of the plant network

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.

Options for improving IT security

SIMATIC offers several options for increasing data and information security and, thus, the security of a production plant. These include:

- Central user administration, staggered user groups and operator rights
- Safety concepts for network security and limited access to network drives
- SIMATIC Security Controller (SSC), ships with WinCC, see chapter "SIMATIC Security Controller (Page 41)"
- SIMATIC NET SCALANCE S firewall and VPN modules

See also

- Chapter "Data and information security (Page 57)"
- All-round protection with Industrial Security - Plant Security, Online Support under entry ID 50203404 (<https://support.industry.siemens.com/cs/ww/en/view/50203404>)
- Manual "Security concept PCS 7 and WinCC (Basic)", Online Support under entry ID 109780811 (<https://support.industry.siemens.com/cs/ww/en/view/109780811>)

3.3 Specification of the basic software

The Software Design Specification (SDS) describes the software's architecture and configuration. This 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. This description serves as a reference when performing subsequent tests (FAT, SAT, etc.).

Commercially available standard software components include automation software components as well as third-party software such as operating system, PDF Reader or Office; see also chapter "Verification of the software (Page 115)".

The following components are described in this manual from the available range of the WinCC system software including suitable options:

Designation	Short description	Additional license required
Configuration Studio	Configuration interface for the following editors	
Alarm Logging	Message archiving	
Tag Logging	Process value archiving	X, if >512
User Administrator	User management in WinCC	
Tag Management	Tag management	
WinCC/User Archives	Setting up user archives	X
Basic Process Control (OS Project Editor, Picture Tree Manager, Time Synchronization, etc.)	Overview diagram and screen navigation, time synchronization	
Graphics Designer	Editor for producing graphics	
Project Duplicator	WinCC tool for copying / duplicating a WinCC project	
Report Designer	Production of reports	
SIMATIC Logon	Interfacing to Windows user administration	
SIMATIC Security Controller	DCOM and firewall settings	
WinCC/Audit	Monitoring of user actions in WinCC Runtime as well as WinCC configurations in the engineering	X
WinCC/Connectivity Pack	External access to archives and messages	X
WinCC/DataMonitor	View of data via the web	X
Performance Monitor	Analysis and optimization of production on the basis of individual performance indicators	X
WinCC/Redundancy	Redundant WinCC server	X
WinCC Server	For the server in a server/client structure	X
WinCC/WebNavigator	View of data and operation of the WinCC project via the web	X
WinCC/WebUX	Mobile operator control and monitoring via the Intranet/Internet.	X
SIMATIC Information Server	Open reporting system with access to archived process values and messages	X
SIMATIC Process Historian	Long-term archiving of process values and messages	X

3.3.1 Operating system

Information on the compatibility of SIMATIC WinCC with the operating systems are included in:

- Product Catalog ST80 (<https://support.industry.siemens.com/cs/ww/en/view/109744146>)
- Compatibility tool (<http://www.siemens.com/kompatool>)
- Online help, readme

The security updates and "critical updates" provided by Microsoft for the Windows operating system are tested by Siemens for compatibility with SIMATIC software and released; see reference in chapter "Updating the system software (Page 132)".

3.3.2 Basic software for user administration

An essential requirement in particular in the GMP field is the access control to the system; which is the only way of ensuring secure operation in compliance with regulations (21 CFR Part 11 and EU GMP Guide Annex 11). Unauthorized access to both the operating and monitoring system as well as the file system and the folder structures in the operating system must be avoided. Appropriate planning is required with this in mind:

- Definition of user groups with various authorization levels for operation and maintenance
- Definition of users and assignment to user groups
- Establishing an adapted system structure, including authorizations of storage folders

Access to the SIMATIC WinCC operator stations is controlled by SIMATIC Logon. SIMATIC Logon supports a user administration system based on Windows mechanisms that can be used both in a workgroup and in a Windows domain. You can find information on installing and configuring SIMATIC Logon in the chapter "Configuration of SIMATIC Logon (Page 47)" and in the SIMATIC Logon Configuration Manual.

3.3.3 Software components for engineering

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 or runtime software (RT) depends on the number of power tags (external tags) required to interface with the automation level.

The Runtime software (RT) is introduced in chapter "Software components for HMI level (Page 28)".

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

WinCC Configuration Studio

The WinCC Configuration Studio offers a clear configuration of the WinCC project data. The user interface is split into a navigation area and a data area oriented on Microsoft Excel.

The WinCC Configuration Studio includes the following editors and functions:

- Tag Management
- Alarm Logging
- Tag Logging
- Text Library
- User Administrator
- User Archive
- Horn
- Picture Tree
- Text and graphic lists
- Menus and toolbars

Tag Management

The external tags (process values) are only maintained in automation systems (PLC) with an absolute and symbolic address. In the SIMATIC S7-1500 series, the querying of tags and PLC data types is based on the symbolic name. This optimizes block access and increases the performance of the S7 program. Tags and PLC data types are transferred to WinCC tag management with the symbol name. Direct transfer is possible with an existing online connection to the PLC. Alternatively, the data is exported to the S7-1500 in the TIA Portal to a file that is loaded in the WinCC tag management. After a change in the PLC in the area of the tags or PLC data types, the data must be updated in WinCC.

With joint project management for the automation systems (S7-300/400) and SIMATIC WinCC in SIMATIC Manager, process tags are maintained centrally in the automation system. SIMATIC WinCC has direct access to the tag symbols in the automation system. The required tags are selected and mapped for display in SIMATIC WinCC. Integration ensures consistency within the project.

3.3.4 Software components for HMI level

The runtime software (RT) is used to control and monitor the production process. The functions for recording and displaying runtime data are described below.

Alarm Logging

Numerous alarms of varying importance occur in a plant. To guide the user, even in critical situations, the alarms of the project are grouped in alarm classes. These alarm classes and a concept for alarm acknowledgment should be defined with the plant operator at the beginning of the project. The entire message system is configured in "Alarm Logging". This includes preparation, display, acknowledgment and archiving of process, system and operator input messages.

Control messages that have been configured in the S7-1500 PLC with message texts and associated values can be loaded in WinCC Alarm Logging. Messages generated in the PLC

are archived with the original time stamp from the PLC in WinCC Alarm Logging and are displayed in the WinCC user interface.

With integration of WinCC and the S7-300/400 automation systems in the SIMATIC Manager, the message texts are maintained in the automation system and taken over by WinCC Alarm Logging.

See also

- Chapter "Creating operator input messages (Page 80)"

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 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

The acquisition and archiving of process data in process value or compression archives is defined in the Tag Logging. These archives form the basis for the long-term archiving of the process data (see chapter "Long-term archiving (Page 30)").

See also

- Chapter "Setup of process value and message archives (Page 91)"

WinCC/Audit

WinCC/Audit is a WinCC option for monitoring user actions in WinCC Runtime as well as changes to the WinCC configuration.

The Audit Viewer allows specific display and analysis of the audit trail. Document Control enables the document management of WinCC screens, scripts, reports and user documents. With the project versioning, you can archive complete WinCC projects and restore project versions.

See also

- System manual "WinCC/Audit", Online Support under entry ID 109818158 (<https://support.industry.siemens.com/cs/ww/en/view/109818158>)

WinCC/User Archives

A concept for structuring recipes should be developed if recipe data or equipment data records are required for ongoing operation. The individual recipe elements can be freely defined for each recipe. A variety of data records can be stored for a recipe. With the WinCC/User Archives option, recipe data or machine data records can, for example, be saved in the form of database tables.

3.3 Specification of the basic software

To obtain an overview of the created data records in an archive, the ActiveX control "WinCC UserArchiveControl" 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 data records can be exported manually in CSV format.

For configuration of operator input messages concerning changes in the data records, see chapter "Setting up user archives (Page 92)".

See also

- WinCC Information System "Options > User Archives"

3.3.5 Long-term archiving

In the regulated environment, relevant production and quality data must be retained in some cases for 5 or 10 years or even longer. It is essential for these data to be defined, reliably saved, and transferred to external archives.

The basic package contains configuration options for archiving. The strategy for exporting to another computer will be defined according to the amount of data accumulated and the retention period.

Long-term archiving of process values and messages can be set up using a long-term archive server, for example, or using the SIMATIC Process Historian option. Both concepts are introduced below.

WinCC long-term archive server

There are options for long-term archiving both in WinCC Tag Logging and in WinCC Alarm Logging. 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.

SIMATIC Process Historian

Process values of multiple WinCC servers (also redundant systems) can be recorded and archived centrally with a SIMATIC Process Historian. Transparent access to the archived data for viewing the messages and process values in the user interface is handled by the system automatically in the background. The messages saved in WinCC archives are fully transferred to the Process Historian. Only those archived process values that are labeled as being "Relevant long term" are transferred.

If the Process Historian is unobtainable, the completed archives remain on the WinCC servers and are transferred later when the link to the Process Historian is reactivated. Allowance should be made for sufficient storage capacity on the SIMATIC WinCC servers. Monitoring of the network connection may also be advisable.

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

See also

- System manual "Process Historian", Online Support under entry ID 109825371 (<https://support.industry.siemens.com/cs/ww/en/view/109825371>)

Batch-based long-term archiving

For the batch-based recording of product-relevant data such as process values and messages, the WinCC Premium Add-on PM-QUALITY can be used (see chapter "Batch-based reporting with PM-QUALITY (Page 36)").

3.3.6 Reporting

For the necessary quality review, a definition is made to establish which production data is relevant for output in a report. A report may contain messages and alarms, recipe data and process values in the form of a table or trend.

Report Designer

The WinCC Report Designer continuously reports process data over a defined period of time. The report output is started via a print job.

The Report Designer is also used for documentation of the configured WinCC project. For this purpose, ready-to-use report layouts and print jobs are provided with SIMATIC WinCC. These can be opened in the Report Designer and modified as required.

Information Server

The SIMATIC Information Server offers the option of reporting on recorded process values and messages. Both pre-configured and those configured based on Microsoft Reporting Services can be represented in the web-based interface and exported to various formats. Additional integration in Microsoft Word, Excel or PowerPoint shows the reports for the archive data in the familiar Office environment.

Batch-based reporting

The WinCC Premium Add-on, PM-QUALITY, offers batch-based reporting of recorded data (see chapter "Batch-based reporting with PM-QUALITY (Page 36)").

Analysis of process values and messages

Based on PM-SERVER process value and alarm logs, PM-ANALYZE can perform evaluations of the number of messages, frequency, etc. as well as statistical evaluations (see chapter "Evaluation and analysis of logs with PM-ANALYZE (Page 37)").

3.3.7 Availability and plant configuration

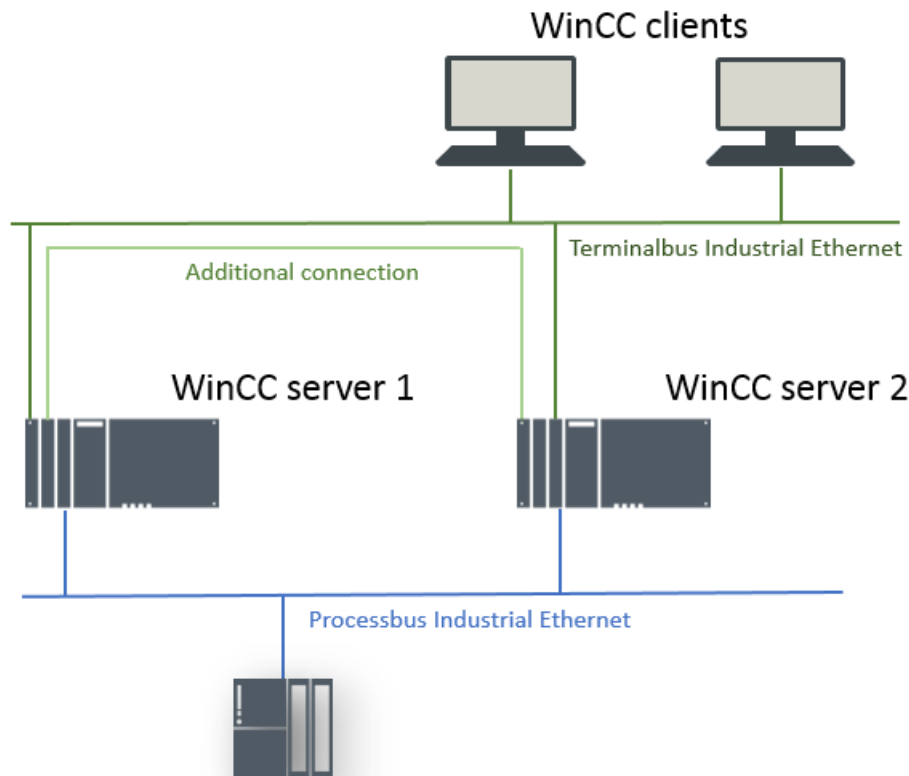
Availability can be increased in an optimum manner by using

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

Availability with WinCC/Redundancy

Redundant archiving of the relevant process values, messages and recipes increases the availability of the data. With the WinCC/Redundancy option, two networked WinCC servers are run in parallel. 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 acknowledgment) and user archives are synchronized directly online.

Once a failed server returns 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/PerformanceMonitor

The WinCC/PerformanceMonitor option is used to calculate and analyze plant-specific key figures for individual devices, machines, or entire production lines.

- 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
- Integration of appropriate display instruments (controls) in WinCC process pictures
- Distribution of evaluations to various people over the web

3.3.8 Interfaces to process data

WinCC/WebNavigator

Remote access to the WinCC project is set up with the WinCC/WebNavigator option. 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/WebUX

The WinCC/WebUX option offers device- and browser-independent remote access to the WinCC project data. The layout and operation of process pictures is subject to restrictions. Remote operation is based on the access control defined in the user administration in the WinCC project. Authorized users must authenticate themselves with a password. The details are checked by SIMATIC Logon.

WinCC/DataMonitor

WinCC/DataMonitor is a pure display and evaluation system for process data from SIMATIC WinCC, or data from the WinCC long-term archive server. 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 & alarms
- Process screens
- WebCenter

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 and/or write access is selected during installation)
- Process tags (states), OPC DA, read and write access, ships with WinCC system software
- Process values, archive values and messages, OPC UA (Unified Architecture), read and limited write access (OPC UA Data Access, OPC UA Historical Data, OPC UA Alarm & Conditions). Requirement for communication via OPC UA is the authentication of the partners by means of certificates.
- All archive data, WinCC OLE DB, or WinCC User Archive with Microsoft OLE DB, read-only access

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

3.4 Application software specification

In addition to the definition of the hardware (see chapter "Selection and specification of the hardware (Page 24)") and the utilized standard software components (see chapter "Specification of the basic software (Page 26)"), the specification of the application software is an integral component of the design specification. Together with the functional specification, the design specification serves as acceptance criteria during system verification (FAT, SAT, etc.).

The design specification can consist of one or more documents. Additional, separate documents are often added as supplements, e.g. process tag list, I/O list, parameter list, P&ID, etc. Like for the other specification documents (URS, FS, DS), the status of these documents (version, release) must be clearly defined.

See also

- GAMP 5 Guide, Appendix D3 "Configuration and Design"

In addition to the previously mentioned hardware specification, the design specification can be divided as follows.

System specification (general)

- System structure, PC profile
- User administration

- Definition of user groups, users, authorizations, local users, configuration of SIMATIC Logon, WinCC user administration, etc.
- Archive configuration (archives, archive cycles)
- Recipe structure
- Interfaces (S7 connections, OPC, discrete I/O processing)
- Printer configuration

HMI design specification

Examples of the aspects specified for the user interface include the following:

- Screen layout and navigation
- Plant pictures, unit pictures, detail pictures of interfaces
- Operator level, access authorizations
- Picture hierarchy
- Screen resolution, picture cycles
- Block icons, graphic elements used
- Alarm classes, priorities, alarm numbering ranges, display

Software design specification

- General information such as name of project, libraries, plant hierarchy
- Software structure, typical and module specification, possibly in a separate document
- Response in the event of power failure and restart
- Time synchronization, specification of time master and slaves
- Description of exceptional states for secure plant operation
- Emergency-off response

3.5 Additional SIMATIC software

This manual introduces the following WinCC Premium Add-ons:

Designation	Short description	Additional license required
PM-CONTROL	Recipe data management and order planning	X
PM-QUALITY	Batch-based data acquisition and logging	X
PM-OPEN IMPORT	Importing process data	X
PM-ANALYZE	Evaluation and analysis of process-value logs and alarm logs	X
PM-LOGON	User logon with RFID card (company ID) using a card reader	X

WinCC Premium Add-ons are enabled with separate licenses.

3.5.1 Batch-based control with PM-CONTROL

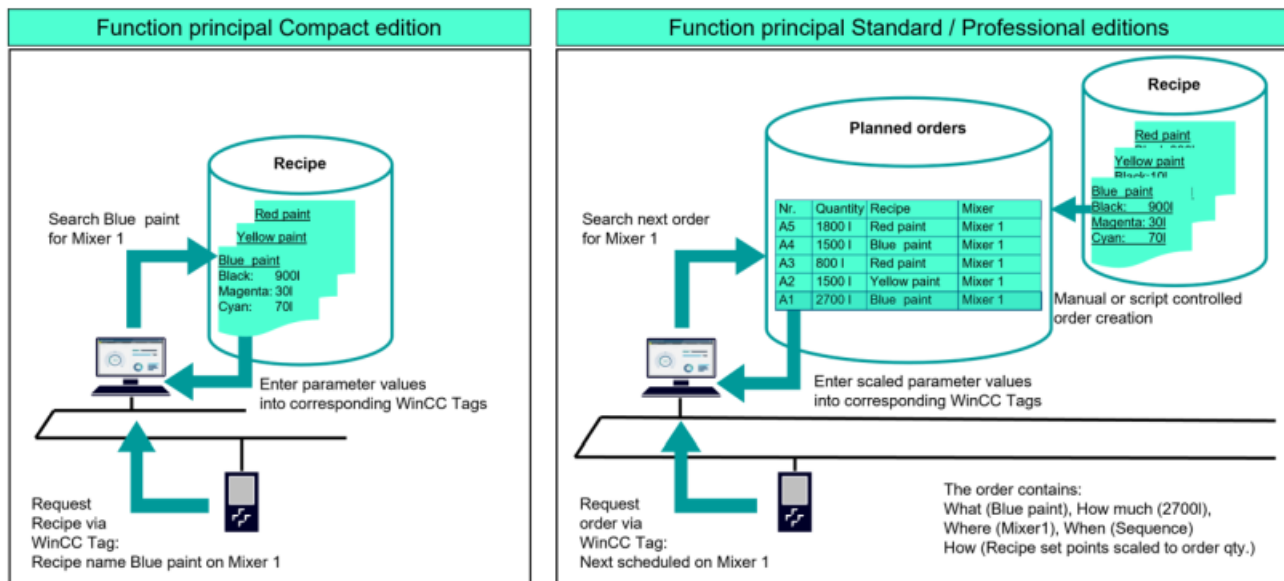
The WinCC Premium Add-on PM-CONTROL is a batch-based parameter control for recipe/product data management. The integrated order control allows flexible handling of production orders in which the recipe, production location, scalable production quantity and the time of production can be specified.

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 with automatic versioning
- Order planning and order control, assignment and management of production orders

The use of SIMATIC Logon as central user administration can be set in PM-CONTROL.

To achieve a cost-effective solution for both simple and more complex tasks, PM-CONTROL is available in the "Compact", "Standard" and "Professional" variants.



3.5.2 Batch-based reporting with PM-QUALITY

The data recorded in the WinCC Premium Add-on PM-QUALITY can be displayed in trends, printed as reports on a printer or exported as an HTML file, XML file or in database format.

The software package includes the following applications:

- Topology Manager for mapping the plant topology and specifying the production data to be acquired such as process values (continuous, snapshot), alarms and operator interventions
- Report Editor for creating the report layout for representation of 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 acquired in parallel in redundant systems

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. It is also possible to use a script in WinCC to configure an electronic signature of the batch report by the logged-on user and with it the manual assignment of the batch status (released / locked).

3.5.3 Batch-based long-term archiving with PM-QUALITY

The batch data acquired with PM-QUALITY can be automatically exported in database format, in HTML format, PDF format and/or in XML format either stored on the local system or on a computer in the network. The PM-QUALITY application Data View (PM-QUALITY Client) can be used to view the batch data exported in database format. The plug-ins for Microsoft Excel provided by PM-QUALITY support tracking and evaluation of batch data.

See also

- Chapter "Long-term archiving (Page 93)"

3.5.4 Importing archives with PM-OPEN IMPORT

With PM-OPEN IMPORT, process data (tag and alarm logs) and operator actions (audit trail) from subsystems are transferred to the databases of WinCC, e.g. archive data from Comfort Panels and HMI devices with WinCC (TIA) Runtime Advanced. This enables the archive data to be centrally compiled and archived in a distributed system with multiple HMI devices. The controls for the trend/table view and alarm view in SIMATIC WinCC are used for viewing the data.

3.5.5 Evaluation and analysis of logs with PM-ANALYZE

PM-ANALYZE supports the analysis and optimization of the production process. Process values and messages of the connected HMI devices are recorded in chronological order and inserted into the alarm and process value archives of the PM-SERVER. These archives form the database for the evaluations and the analysis functions in PM-ANALYZE.

Convenient filter settings for filtering messages by message content and time range as well as statistical analyses by volume and frequency reveal errors and weak points. PM-ANALYZE offers a wide range of charts for displaying logged process values, from dot, stair or curve lines to bar and pie charts. The special feature of PM-ANALYZE is the parallel display of charts and messages in a workspace. Alarms in tables and in statistical evaluations parallel to process values in charts show the range of production data at a glance, even with large amounts of data.

The PM-ANALYZE add-in for Microsoft Excel offers access to process value and message archives as well as extensive statistical evaluations of the process values.

3.6 Utilities and drivers

3.6.1 Printer drivers

It is advisable to use the printer drivers integrated in the operating system and approved for WinCC. If external drivers are used, no guarantee of proper system operation can be provided.

3.6.2 Virus scanners

The use of virus scanners is enabled in process mode. The enabled virus scanners can be accessed via the compatibility tool (<http://www.siemens.com/kompatool>) in the product support.

The following settings must be taken into consideration when using virus scanners:

- The real-time search is one of the most important functions. It is sufficient, however, to restrict the analysis to incoming data traffic.
- Scheduled scans must be deactivated, as they significantly limit system performance in process mode.
- The manual search may not be run during process mode. It can be performed at regular intervals, e.g. during maintenance cycles.

These arrangements should be described in the specification and/or where necessary, in a work instruction (SOP) from the IT department in charge.

3.6.3 Image & partition tools

Supplemental "Imaging" and "Partitioning" software allows you to create a backup of the entire contents of a hard drive, the so-called image, as well as to partition the hard drives. The system software backed up in the image can be used to quickly restore a system. Backed up hard drive contents can also be imported to devices of the same type. This facilitates the replacement of computers.

Siemens provides the software package "SIMATIC Image and Partition Creator" to perform these tasks. This is possible without a separate installation. Administration skills are required.

See also

- SIMATIC IPC Image and Partition Creator, Online Support under entry ID 109781271 (<https://support.industry.siemens.com/cs/ww/en/view/109781271>)

Note

The created images are used to restore the installed system, but not to back up online data, user software (project), as well as authorizations and license keys.

Detailed information on the topics of data backup and system restoration is included in the respective chapters of this manual.

System Installation and Basic 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-station 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. The WinCC RT Client license is suitable for a standard client without a project and with a view of a WinCC server. In a distributed system configuration clients show the user interface of several WinCC servers. These clients have their own project and are licensed with the smallest WinCC RT license.

4.1 Installation of the operating system

Panel PCs are available in different expansion stages with installed operating system. The hardware and operating system requirements of the SIMATIC HMI software must be taken into consideration when using standard PCs. Details can be found in the current product catalog. Current information on the operating system installation can be found in the WinCC Information System in the chapter "WinCC Installation Notes > Installation Requirements".

Note

The computer name must conform to the naming convention of the SIMATIC software application. You should read the information in the respective installation instructions and Readme files of the SIMATIC software to be installed on the computer, e.g. SIMATIC Net.

The computer name may no longer be changed after the SIMATIC WinCC system software is installed. This would require a complete re-installation of the system software.

See also

- System manual "WinCC Information System", Online Support under entry ID 109824651 (<https://support.industry.siemens.com/cs/ww/en/view/109818193>)
- WinCC Information System > Working with WinCC > Annex > Impermissible Characters

4.2 Installation of SIMATIC components

SIMATIC WinCC can be installed as a stand-alone component or installed integrated in the SIMATIC Manager. Both variants have advantages that are described briefly.

4.2 Installation of SIMATIC components

The use of the SIMATIC Manager as the central configuration interface unites the automation level and the HMI system in a common project. This results in the following advantages:

- Simple transfer of tags and texts to the WinCC project
- Direct access to STEP 7 symbols during process connection
- Project-specific access protection (STEP 7 and WinCC)
- Extended diagnostics support

If redundant systems are used:

- Simple administration for master and standby server
- Complete download and downloading changes online for master and standby server

See also

- System manual "Working with WinCC", chapter 17, Online Support under entry ID 109824649 (<https://support.industry.siemens.com/cs/ww/en/view/109818253>)
- WinCC Information System > Working with WinCC > Integration in the SIMATIC Manager

The SIMATIC Manager also offers additional helpful options for automation and project management:

- Programming with CFC, including type/instance concept
- Version Trail for version management of the entire project
- Version Cross Manager for comparing two versions of the automation project

It must be noted that the SIMATIC Manager is only suitable for configuration of the automation systems SIMATIC: S7-300 and S7-400, however not for the SIMATIC S7-1200/1500 series, which are configured via the TIA Portal. The S7-1500 in particular also offers the advantages of integrated engineering which are mentioned in this manual in chapter "Connection to SIMATIC S7 (Page 109)".

4.2.1 SIMATIC WinCC

Note

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

Central installation

The record function simplifies the installation of the same WinCC system on multiple computers. A WinCC installation is performed and recorded in the Ra-Auto.ini control file. Only the control file is started on the other PCs. The prerequisite is that the computers are equipped with the same operating system.

See also

- WinCC Information System > WinCC V8.0 Installation Notes / Release Notes > Installing WinCC > Configure automatic installation of WinCC

Service mode

The SIMATIC WinCC system software can be operated in service mode if the WinCC Server is not intended for control of the process in a distributed system with server and clients. This means that the logon of a Windows user on the WinCC Server is not required but is possible for service interventions. The WinCC Project that is automatically started and activated when the computer is started is configured in Autostart.

This mode is suitable for WinCC Servers that are located in a remote server room and/or are operated in a virtual environment.

Note

The PM products PM-CONTROL, PM-QUALITY, PM-ANALYZE, and PM-LOGON require a registered Windows user for operation and are therefore not released for service mode.

See also

- WinCC Information System > Configurations > WinCC Service Mode

WinCC in a virtual environment

The SIMATIC WinCC system software is released for operation in a virtual environment. The approved virtualization systems are listed in the WinCC information system. The specified entry ID contains additional information.

See also

- WinCC Information System > WinCC V8.0 Installation Notes / Release Notes > WinCC Installation Notes > WinCC installation requirements > Hardware requirements for installing WinCC
- WinCC Virtualization, Online Support under entry ID 49368181 (<https://support.industry.siemens.com/cs/ww/en/view/49368181>)

4.2.2 SIMATIC Security Controller

During installation of the WinCC system software, default settings in the Windows operating system have to be adapted to the requirements of the WinCC software. For SIMATIC WinCC, the required settings in the operating system are managed in the SIMATIC Security Controller application. The application can be opened via Start > Programs > Siemens Automation > Security Controller and clearly displays the settings that are made. An option for saving and printing is offered.

4.3 Setting up user administration

The following settings are automatically configured for specific functions:

- Required Windows user groups
- Security-related registry entries
- Configuration of the Windows firewall exception list
- DCOM settings (Distributed Component Object Model)
- File system rights

SIMATIC Security Controller is restarted automatically if additional settings in the Windows operating system are required after installation of WinCC options, such as the WinCC/ WebNavigator option.

Note

If the WinCC computer is included in another working environment (domain or workgroup), the settings must be reconfigured by the SIMATIC Security Controller.

The settings are documented in XML format.

4.2.3 SIMATIC WinCC options

Additional 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 WinCC File Server is installed on this computer. For Alarm Logging and Tag Logging, the target paths are configured in such a way that the closed archive files are saved on this computer (see chapter "Long-term archiving (Page 30)").

See also

- WinCC Information System > Configurations > File Server > File Server Setup

4.3 Setting up user administration

For secure operation in compliance with regulations, controlled access to both the operating level and configuration level as well as archive data and backup copies is required.

A user-related logon and logoff for operator actions is one of the basic functionalities for meeting this requirement.

The user management of SIMATIC Logon uses the mechanisms of the Windows operating system and therefore ensures reliable access protection. For the organization of operating authorization, the users are assigned their tasks according to various user groups in the Windows user administration.

These user groups are assigned authorizations for the individual operator actions.

Note

The structure of the user groups should already be defined in the specification at the start of the project and be set up at the start of the configuration phase.

All authorization levels for operator control elements on the visualization interface (faceplates, input boxes, buttons, etc.) and their assignment to user groups must be set up according to specifications and tested in the course of the project.

The setup is differentiated in terms of which level the user operates. The affiliation to certain Windows user groups is therefore required for the start or the configuration of SIMATIC components such as SIMATIC WinCC or SIMATIC Logon. These user groups are automatically created in the Windows user administration upon installation of the software components and must not be deleted.

For the operation of process mode, project-specific user groups are set up which are equipped with the required operation permissions in the configuration.

The following sequence is recommended when setting up user administration with SIMATIC Logon and is described in the following chapters:

- Setting up user groups and users at operating system level, see chapter "User administration on the operating system level (Page 44)"
- Setting up security settings in Windows, see chapter "Security settings in Windows (Page 45)"
- SIMATIC user groups, see chapter "SIMATIC user groups (Page 46)"
- Setup and configuration of SIMATIC Logon, see chapter "Configuration of SIMATIC Logon (Page 47)"
- Administration of authorizations for the individual user groups, see chapter "Administration of authorizations (Page 50)"
- Assignment of the authorizations for individual objects as part of the configuration (picture windows, input boxes, operating buttons)

Note

The implementation of user management based on SIMATIC Logon and Microsoft Windows Administration is recommended both in distributed systems (also in conjunction with Panels) and for single-station systems.

SIMATIC Logon is included in the scope of delivery of the SIMATIC WinCC software.

4.3.1 User administration on the operating system level

Administration of user permissions using SIMATIC Logon is based on the mechanisms of the Windows operating system. Two user administration options are available here:

- Centralized administration in a **domain structure**
- Management on a computer of a **workgroup**

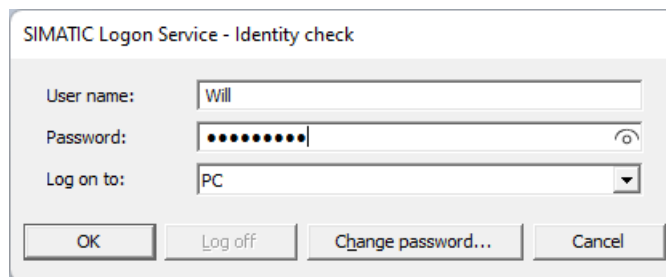
When using multiple servers or when there are redundant servers, a domain structure must be set up to ensure that users will still be able to perform operations and log on even if one domain server fails. However, the domain server functionality may not be installed on the WinCC system.

Note

The complete name for each user must be entered under "Local users and groups" in the Windows Computer Management. This name can be used for display in SIMATIC WinCC after logging on and is required for electronic signatures. The full name must therefore be specified.

See also

- Operating system help of Microsoft Windows or the appropriate Windows manual (for setting up Windows workgroups and the domain)
- WinCC Information System > Working with WinCC > Setting up User Administration
- System manual "Working with WinCC", chapter 15, Online Support under entry ID 109824649 (<https://support.industry.siemens.com/cs/ww/en/view/109818253>)
- Manual "Security concept PCS 7 and WinCC (Basic)", chapter 6.4.1, Online Support under entry ID 109780811 (<https://support.industry.siemens.com/cs/ww/en/view/109780811>)



While a user is authenticated for his operator rights in the SIMATIC environment when he logs on, a "default user" is always logged on to the operating system in parallel and has the permissions required for the operating system level. These should not be higher than required for operation, see also chapter "Access control to operating system level (Page 52)".

Note

The user logged on to the operating system must be the same throughout the entire system; he must be logged on automatically when a computer starts up. Excluded are WinCC servers that are operated in service mode. If having the same Windows user is not desired, the users must at least be known on all computers in the system group.

Windows domain

The one-time administration of groups and users on a domain server reduces the maintenance work and provides greater security. All computers in the domain are admitted as members of the group.

Note

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

Windows workgroup

In a workgroup, all the groups and users are created and managed on the workgroup, against which SIMATIC Logon checks the logon data.

Note

To prevent the failure of the central logon server, it is recommended to create the required Windows groups and Windows users on a second computer (e.g. the local computer). In the event of an error, the logon computer can be changed in the logon dialog.

4.3.2 Security settings in Windows

Access authorizations as well as settings such as the length, complexity, and validity period of the password can and should be configured appropriately to increase data security.

When SIMATIC Logon is used, the system administrator configures the following security settings in Windows under "Control Panel > Administrative Tools > Local Security Policy > Security Settings > Account Policies / Local Policies" (depending on the Windows operating system):

- Password policies such as complexity, password length, password aging
- Account lockout policies
- Audit policies (e.g. logon events and logon attempts)

Note

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

See also

- Chapter "Disabling the operating system level during operation (Page 55)"
- Manual "PCS 7 Compendium Part F – Industrial Security", chapter 7.4 "Password policies", Online Support under entry ID 109815443 (<https://support.industry.siemens.com/cs/ww/en/view/109815443>)
- All-round protection with Industrial Security - Plant Security, Online Support under entry ID 50203404 (<https://support.industry.siemens.com/cs/ww/en/view/50203404>)

4.3.3 SIMATIC user groups

SIMATIC WinCC supports the Windows permissions model.

When the WinCC server software is installed, SIMATIC standard user groups with different permissions are automatically created in the operating system (SIMATIC HMI, etc.). These must not be changed or deleted. With these user groups, access authorizations for the user logged on in Windows are controlled by the SIMATIC WinCC system software.

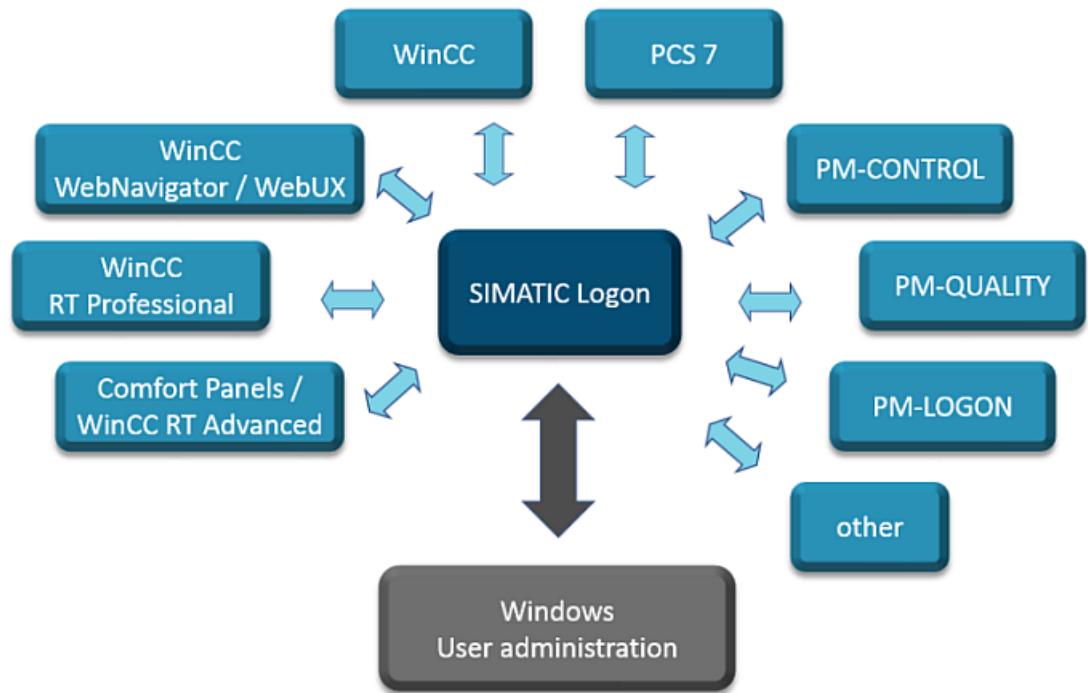
By differentiating between system administrators and users (plant operators) at the Windows level logon, a logical separation is achieved for the computer access authorization. A simple Windows user with rights of the "Users" user group is sufficient for operation of SIMATIC WinCC.

See also

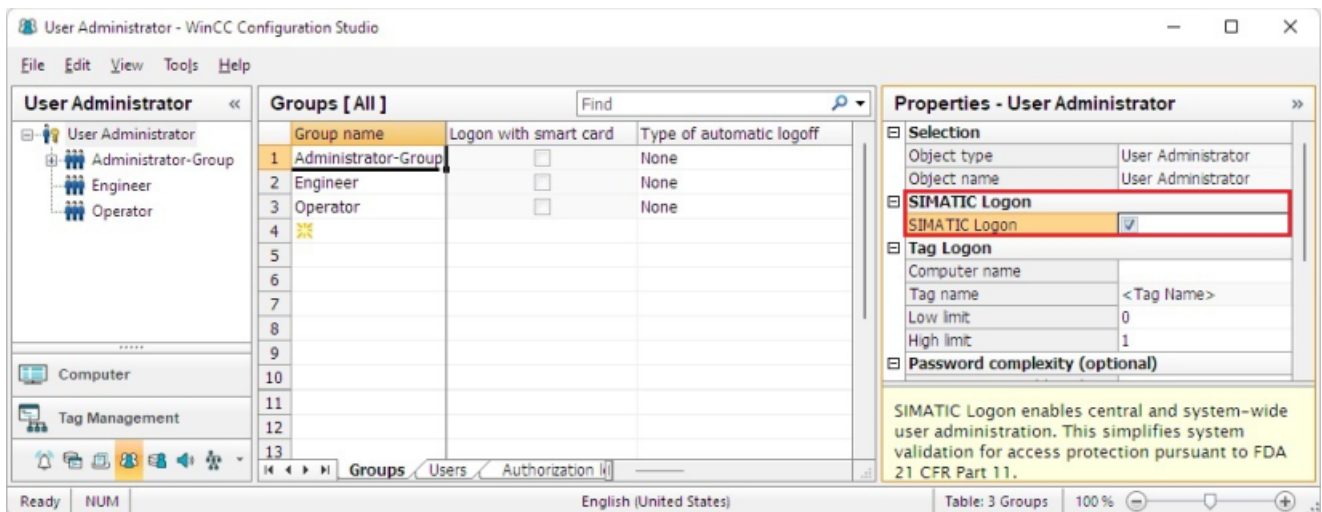
- Chapter "Access control to operating system level (Page 52)"
- WinCC Information System > WinCC V8.0 Installation Notes / Release Notes > WinCC Installation Notes > Requirements for the installation of WinCC > Specifying access rights in the operating system

4.3.4 Configuration of SIMATIC Logon

SIMATIC Logon serves as an interface between Windows user administration and the SIMATIC components. It checks the correctness of logon data for a user against the central user administration. If the logon is valid, the associated user groups are returned to the operator station. The logon of users for the operation of WinCC options and Premium Add-ons can be included in the check by SIMATIC Logon.



The basic use of SIMATIC Logon is activated in the User Administrator properties in the WinCC Explorer. The WinCC Configuration Studio automatically opens the relevant configuration interface.



4.3 Setting up user administration

The basic settings of SIMATIC Logon are made in the "Configure SIMATIC Logon" dialog. The settings are described in the SIMATIC Logon configuration manual and include, for example:

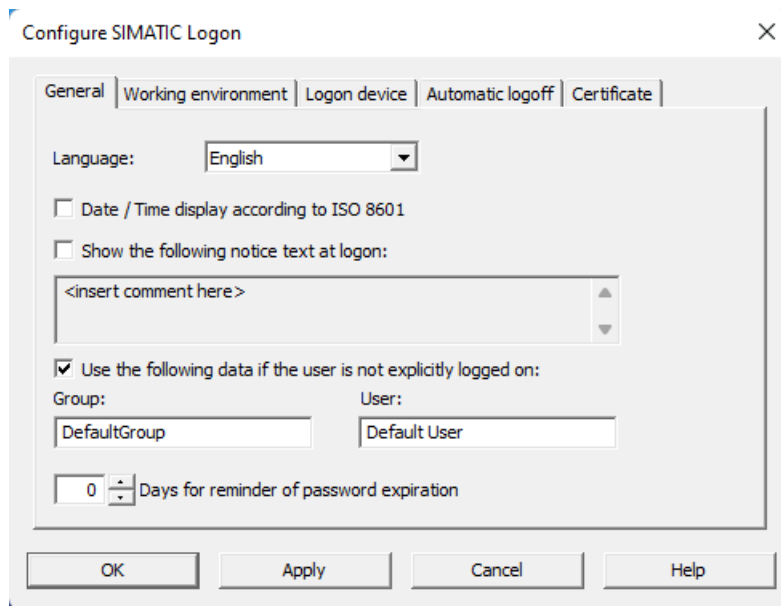
- The logon of a "default user" after a user logoff
- Logon server ("working environment")
- Automatic logoff on using SIMATIC Logon

Default user after user logs off

In the "General" tab, you can define whether a default user should be logged on after a user logs off.

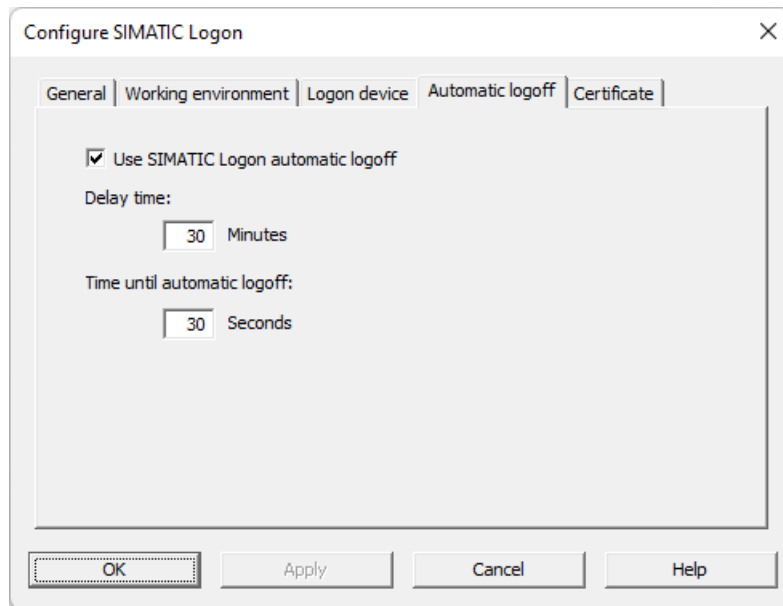
Unlike all other users, the "Default User" user does not have to be created as a Windows user. The "Default user" is a member of the "Default group" or another user group assigned here. The rights of this group are defined in the WinCC User Administrator.

Caution: In any case, the Default User can carry out the operator actions for which no operator right has been defined.



Automatic logoff (Auto Logoff)

To prevent unauthorized accesses from occurring with the logged-on user, the "Auto Logoff" function should be enabled and a time assigned in the SIMATIC Logon configuration. If the use of the Default User was enabled, he will then be logged on.



Note

The "Automatic logoff" function, however, must not be enabled at the operating system level, as this will close down the user interface completely.

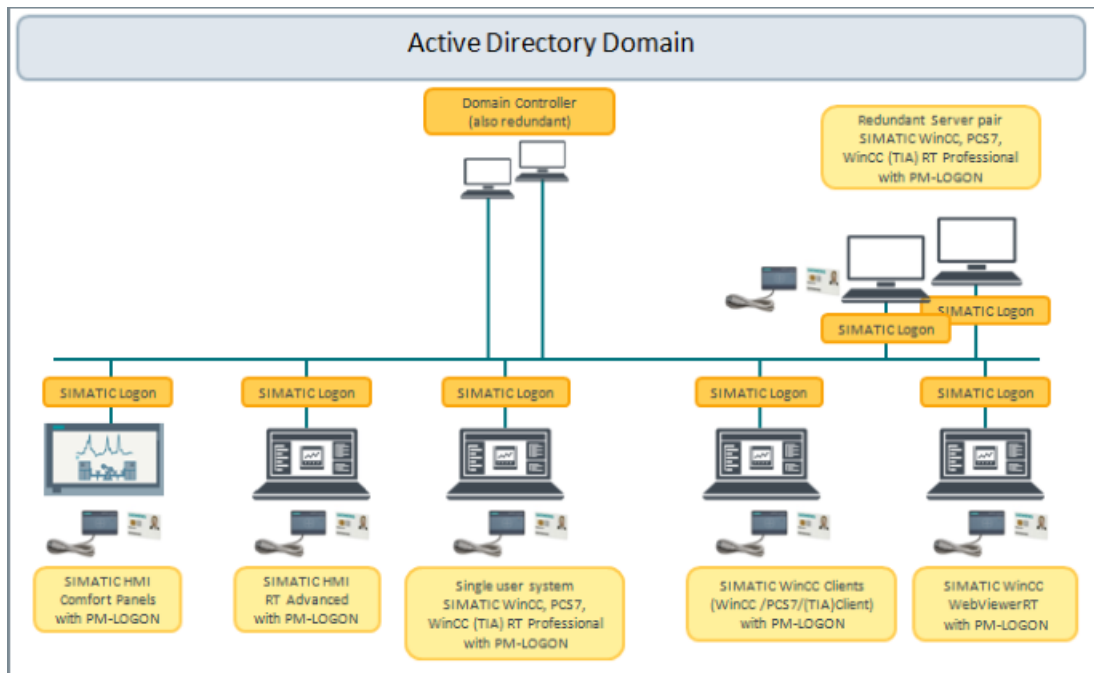
A screen saver must also be disabled when SIMATIC Logon is used. Otherwise, when unlocking the screen, the system would ask for the password of the Windows user, which the WinCC operator should not know.

4.3.5 Logon via RFID card reader with PM-LOGON

The Premium Add-on PM-LOGON offers users a secure and convenient logon with the company ID using a card reader on the HMI device.

Depending on the HMI device, PM-LOGON performs logon through various services (SIMATIC Logon, WinCCViewerRT or OPC and SOAP Access).

The users and user groups are managed in the Active Directory of a domain or in a Windows workgroup. The ID of the ID card is stored together with the encrypted password for the user. Reading the ID on the card reader starts a data query via SIMATIC Logon. The data query provides the user name with which the PM-LOGON Runtime logs the user on to the HMI device. The application supports various card readers. The card readers are not included in the scope of delivery.



See also

- Information about PM-LOGON on the Internet (<https://www.siemens.com/process-management>)

4.3.6 Monitoring access protection

Events, such as successful and failed logons and logoffs or password changes are stored both in the EventLog database of SIMATIC Logon and in WinCC Alarm Logging. These events can be viewed and exported via the SIMATIC Logon Eventlog Viewer.

Changes to the user and user group configuration are recorded in the Windows EventLog at operating system level and can be backed up there.

See also

- Chapter "Audit trail and change control (Page 84)"

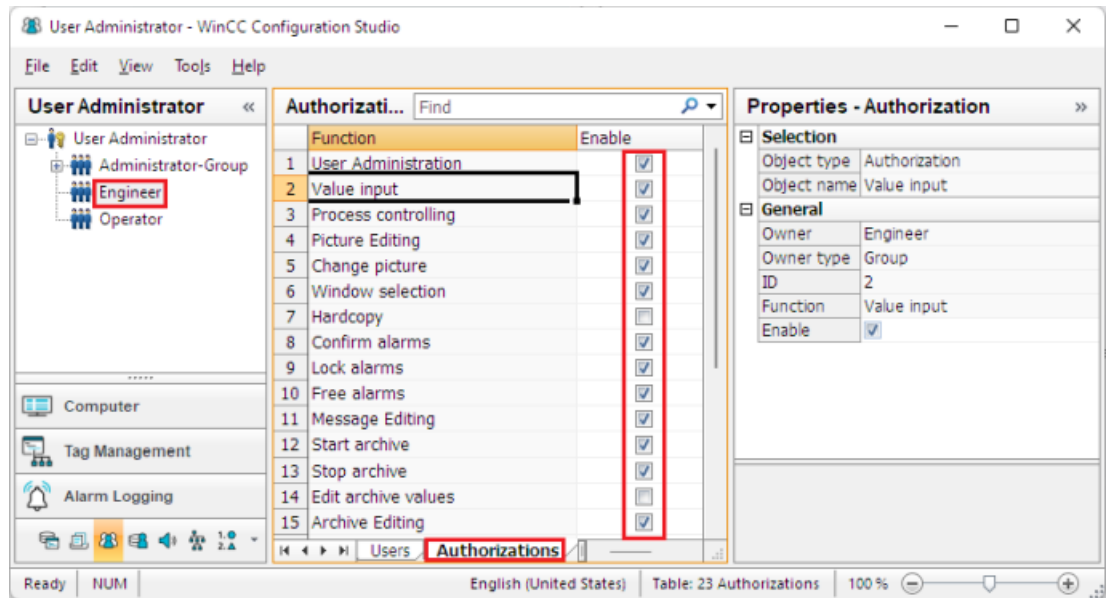
4.3.7 Administration of authorizations

The authorizations in the WinCC user interface are always assigned to the project-specific user groups. For this purpose, the required user groups are created in WinCC Configuration Studio in the User Administrator view with the same names as the user groups in Windows. Name matching is required for checking of the logon data by SIMATIC Logon.

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



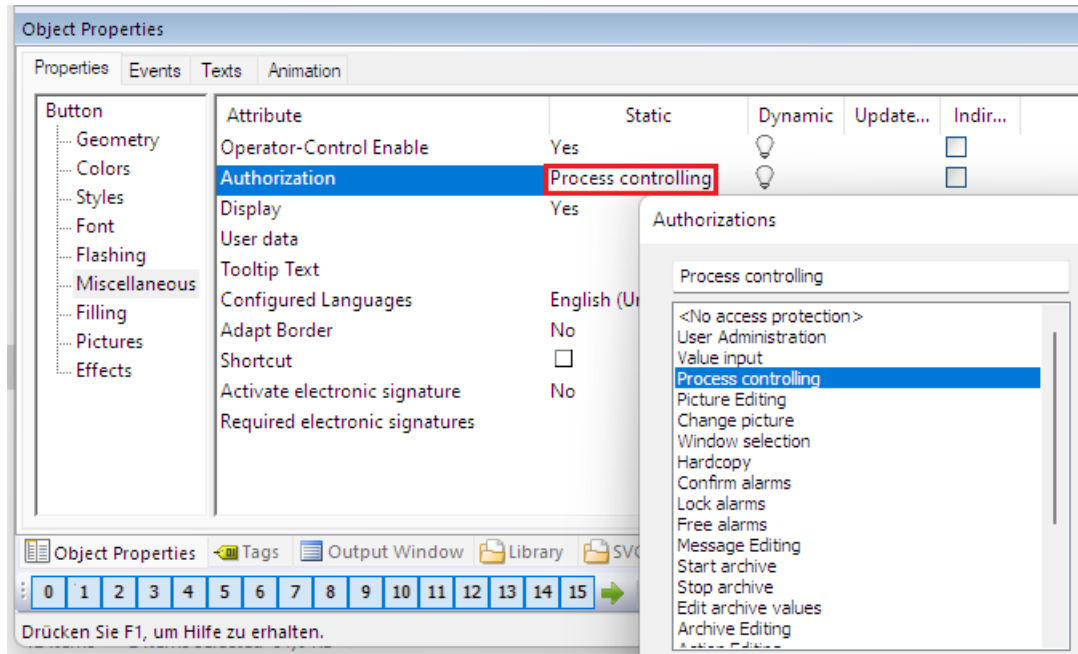
The permissions for the group members are assigned via the user groups in the WinCC project. Here in the screenshot, for example, the appropriate rights are assigned to users who are members of the Windows group "Engineer".

See also

- WinCC Information System "Working with WinCC" > Setting up User Administration
- Chapter "Configuration of SIMATIC Logon (Page 47)"

4.3.8 Assigning authorizations

SIMATIC WinCC provides a series of objects for creating the user interface. Objects which offer operator control in process mode, such as I/O field, button, slider object, bars, controls and many more can be protected with an authorization. This ensures that only a logged-on user with the appropriate authorization can perform an operation.



The operation of the WinCC controls can be protected for every button in the toolbar with an authorization.

Note

It should be ensured that the button for ending process mode (deactivate runtime) can only be operated by authorized personnel.

4.4 Access control to operating system level

For the operation of WinCC Runtime or the remote access to a WinCC project, simple user rights are sufficient for the Windows user logged on in the background. The user must be a member of the "User" Windows group and the SIMATIC HMI group, see chapter "SIMATIC user groups (Page 46)".

This ensures that only the SIMATIC WinCC system software has access to the SQL database. Accesses by the operating system to the SQL database are therefore not possible.

Note

In a distributed system with several operator stations, the same user should be logged on everywhere in the Windows operating system. This must be taken into account during automatic startup.

For the plant operator logged on in WinCC Runtime, on the other hand, access to the operating system level is not required and usually not desired. Additional configuration settings (startup characteristics, disabling the operating system level) must therefore be made. These settings avoid unauthorized access from the SIMATIC WinCC user interface to sensitive data of the operating system.

Note

Access to the operating system level should be reserved exclusively for administrators and technical maintenance personnel.

See also

- WinCC Information System > WinCC V8.0 Installation Notes / Release Notes > WinCC Release Notes > Notes on operation > Information on the Windows operating system > Preventing access to Windows in runtime
- Disabling shortcut keys, Online Support under entry ID 44027453 (<https://support.industry.siemens.com/cs/ww/en/view/44027453>)
- Chapter "Security settings in Windows (Page 45)"

4.4.1 Startup characteristics

For the secure start of the operator station, automatic startup is configured until activation of the user interface. Access to the operating system level is therefore prevented during startup.

The automatic logon (Auto-Logon) in the Windows operating system in a workgroup or domain is described in the Online Support under entry ID 23598260 (<https://support.industry.siemens.com/cs/ww/en/view/23598260>) as an example.

Automatic startup of WinCC Runtime

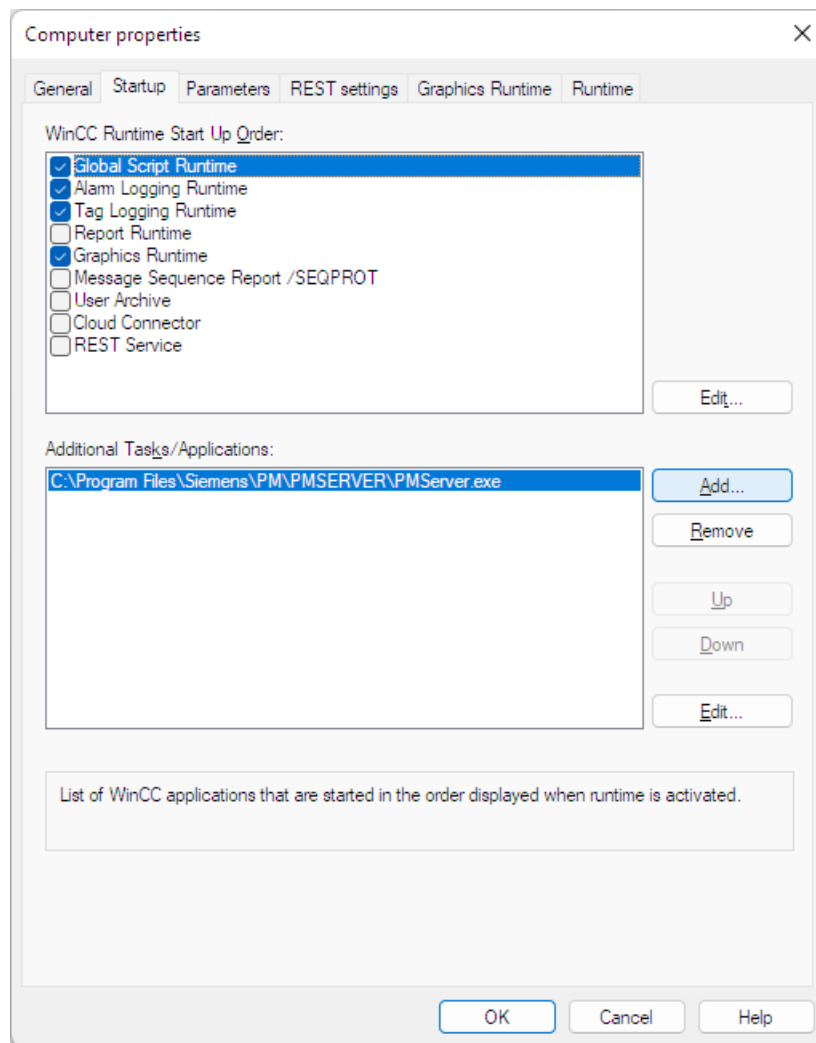
Automatic startup is organized in the "Autostart" application. This is opened via the Windows Start menu > Siemens Automation > Autostart.

Through the function "Disable operating system access on startup", a WinCC splash screen is shown immediately which can also be designed individually.

- WinCC Information System > Working with WinCC > Working with Projects > Activating Project > How to Set Up Autostart

When the "Autostart active" property is activated, the specified project is opened in WinCC Explorer when the computer is started up. If the runtime was activated when the project was exited, it is automatically reactivated. The property "Allow "Cancel" during activation" should not be selected to ensure that the project start cannot be interrupted.

The services which are required during operation are activated under Computer properties > Start. Other applications that should be started automatically, such as the Premium Add-ons PM-CONTROL or PM-QUALITY, are added under "Additional tasks / applications".

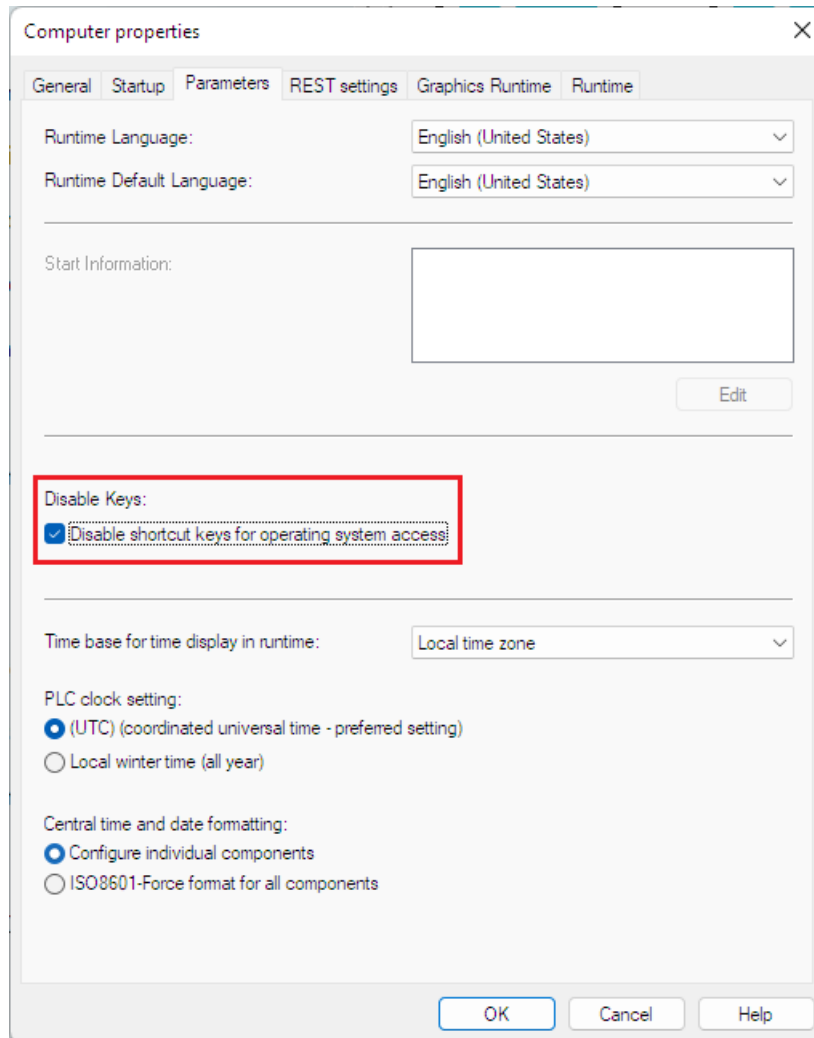


4.4.2 Disabling the operating system level during operation

For security reasons, access to the Windows operating system level is only permitted for administration and maintenance personnel. Additional configuration settings are required for this purpose. These settings avoid unauthorized access from the process mode of SIMATIC WinCC to sensitive data of the operating system.

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 authorizations. After deactivation, the operating system can be accessed.

See also

- Disabling key combinations, Online Support under entry ID 44027453 (<https://support.industry.siemens.com/cs/ww/en/view/44027453>)
- WinCC Information System > WinCC V8.0 Installation Notes / Release Notes > WinCC Release Notes > Notes on operation > Information on the Windows operating system

Preventing system access during object programming

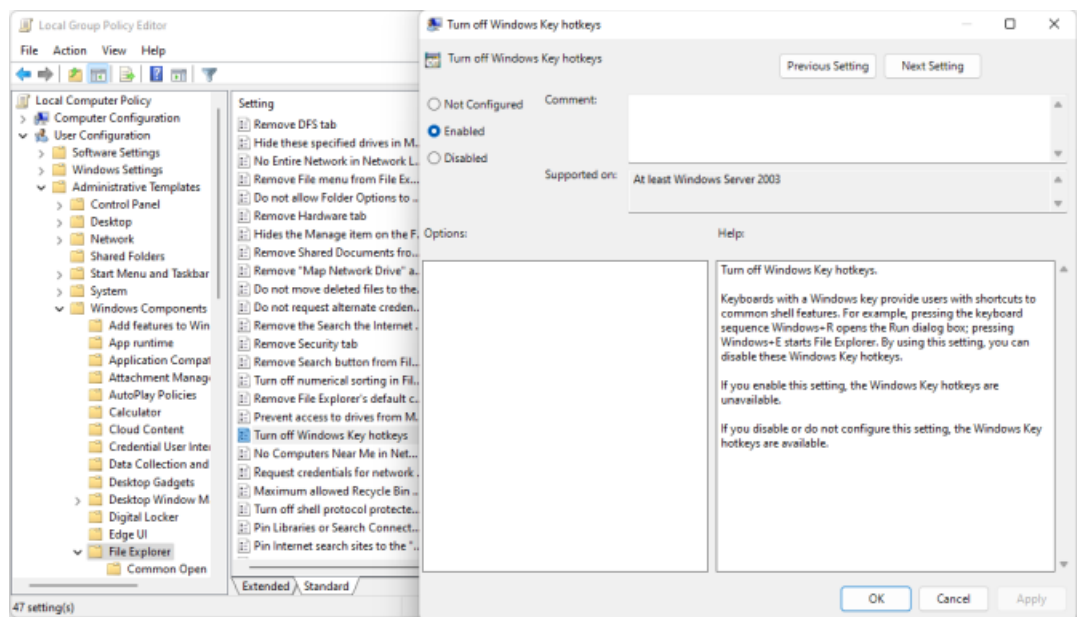
Make sure that no objects are used in the user interface that permit access to the Windows file system or to executable programs. This risk exists, for example, with OLE objects, Internet links, online help system etc.

Configuration settings in Windows

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

The Cortana voice commands should also be disabled.

In addition, it must be ensured that any shortcut key assignments are deactivated to prevent access to the operating system interface.



See also

- WinCC Information System > WinCC V8.0 Installation Notes / Release Notes > WinCC Release Notes > Notes on operation > Information on the Windows operating system > Preventing access to Windows in runtime

4.5 Data and information security

In the regulated environment, production processes and recorded data are subject to control and secure retention to ensure verification of product quality. The secure handling of data is a basic requirement for operation in compliance with regulations.

National and international regulations require retention of relevant production data and operator inputs for many years. For this reason, there are many facets to data and information security, some of which are described here.

Definition of a suitable system structure

- User administration, see chapter "Setting up user administration (Page 42)"
- Planning of data storage and of input and output devices
- Secure storage of sensitive data with redundancy and access protection
- Using virus scanners, see chapter "Virus scanners (Page 38)"
- For defined behavior on startup and when operating the user interface, see chapter "User administration on the operating system level (Page 44)"

Organizational measures

- Planning and assignment of the required access permissions
- Supplementation by codes of behavior, e.g., for handling of USB sticks
- Work instructions for archiving, reading back, and possibly data migration

Adapting the operating system settings

When SIMATIC WinCC is installed, settings in the operating system are checked against the software requirements with SIMATIC Security Controller and adapted, see chapter "SIMATIC Security Controller (Page 41)".

Plants and terminal bus

Industrial Ethernet offers a comprehensive range of network components for electrical and optical data transmission technology. In SIMATIC WinCC, you can differentiate between plant bus and terminal bus. To guarantee a high degree of security and performance, it is advisable to install these two buses separately.

Industrial Ethernet is used as the plant bus. The automation systems are connected to the WinCC servers via the plant bus.

WinCC servers, WinCC clients, archive servers and higher-level MES systems, if any, communicate via the terminal bus.

See also:

- Manual "PCS 7 Compendium Part A", chapter 4.3.6 "Configuring the terminal bus" or chapter 4.3.7 "Configuring the plant bus", Online Support under entry ID 109809015 (<https://support.industry.siemens.com/cs/ww/en/view/109809015>)

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

- Information about the products of the SCALANCE family (<https://www.siemens.com/us/en/products/automation/industrial-communication/scalance.html>)
- Protection of an automation cell by the SCALANCE S security modules via firewall, Online Support under entry ID 22376747 (<https://support.industry.siemens.com/cs/ww/en/view/22376747>)

Defense in depth

The concept of "Defense in depth" requires measures on various levels to establish plant security, network security, and system integrity.



The experts of the Industrial Cybersecurity Services (<https://www.siemens.com/us/en/products/services/digital-enterprise-services/industrial-security-services.html>) are happy to provide support with the design of a security concept.

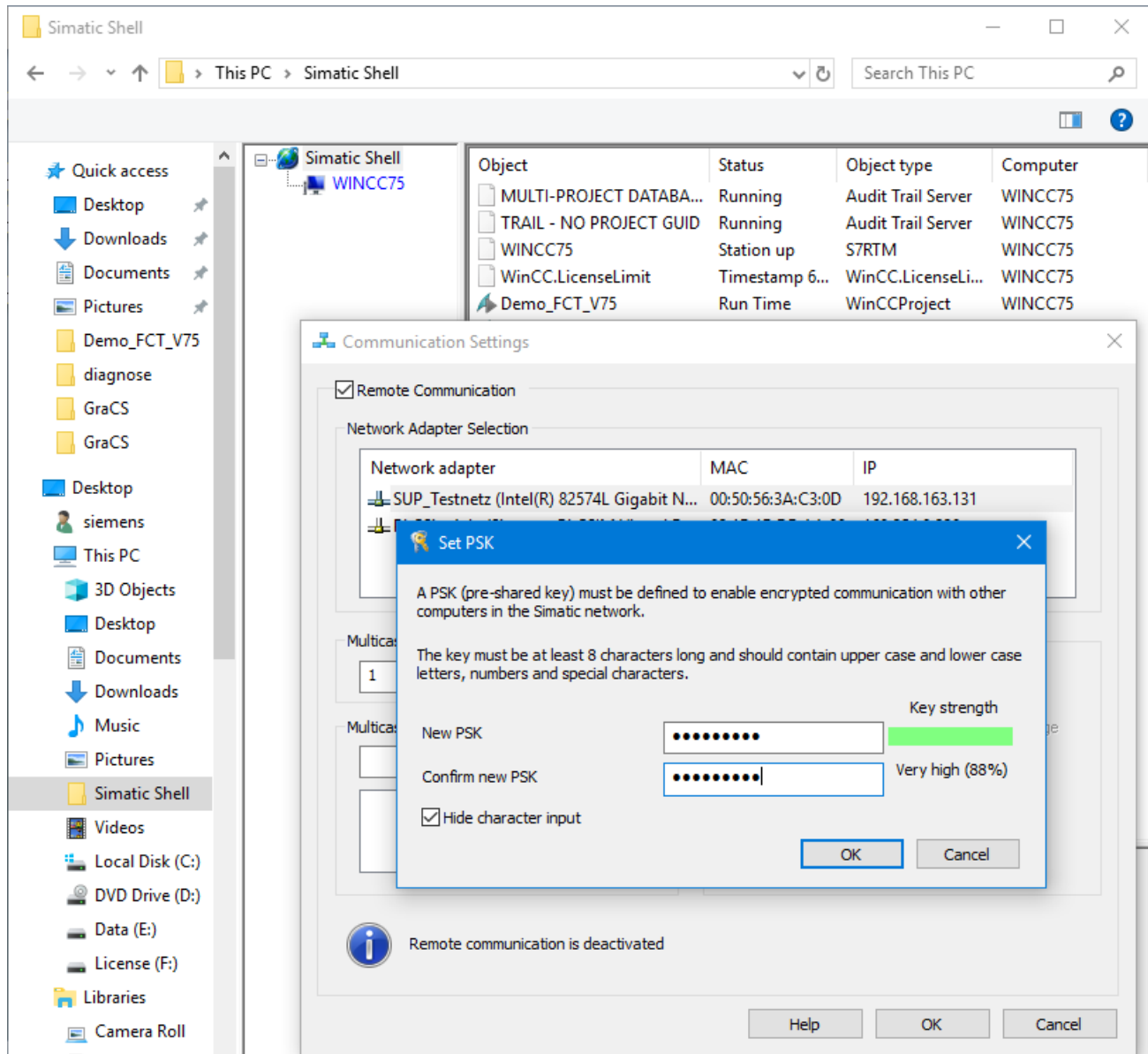
See also:

- Comprehensive information on the topic of "Industrial Security", Online Support under entry ID 50203404 (<https://support.industry.siemens.com/cs/ww/en/view/50203404>)

SSL encryption in distributed systems

Communication between WinCC server and WinCC clients in distributed systems is performed in the network with SSL encryption. For this purpose, the remote connection must be explicitly enabled in the SIMATIC Shell network administration and a PSK key must be defined on each computer. Only computers with the same PSK key can communicate with each other.

Different environments in a network can be set up each with its own PSK key.



Security by default

As of WinCC V7.5, security in communication is enhanced by default. This applies to new installations and upgrades.

- In the communication settings under SIMATIC Shell, "Remote Communication" is disabled and must be actively enabled for redundant systems or multi-station systems. The SSL encryption is automatically enabled.
- Write access is disabled for shared WinCC project folders.
- The WinCC options WebUX and Cloud Connector support encrypted communication only.
- Improved access protection to the WinCC databases, see WinCC Release Notes

See also

- WinCC Information System > Getting Started > What is new in WinCC V8.0? > Function extensions in case of safe operation of the plant (chapter 2.1.4)
- WinCC Release Notes, notes on the database in chapter 1.2.2.3, Online Support under entry ID 109818202 (<https://support.industry.siemens.com/cs/ww/en/view/109818202>)

WinCC Certificate Manager

WinCC follows the strategy "Security by default" to support in the configuration of plants and systems.

With the "WinCC Certificate Manager" application, you create a WinCC Certificate authority and the WinCC certificates required for the PCs. The certificates are distributed to the PCs and installed there. The Certificate Manager also supports with establishing the relationship of trust between Runtime and its communication partners.

WinCC supports the use of CA-based certificates (CA = Certificate Authority) in runtime.

Additional security measures

Additional protective measures should be considered when selecting products and systems as well as when designing production plants. These include:

- Antivirus, see All-round protection with Industrial Security, Online Support under entry ID 92605897 (<https://support.industry.siemens.com/cs/ww/en/view/92605897>)
- Application Whitelisting with McAfee Application Control, Online Support under entry ID 88653385 (<https://support.industry.siemens.com/cs/ww/en/view/88653385>)
- Automation Firewall
- Industrial Anomaly Detection
- Security Awareness Training

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 Project setup

5.1.1 Creating a project

For the effective creation of a WinCC project, the project type (single-user station or multi-user station), project path and naming conventions are considered during planning. A definition of prefixes for tags, screens and functions can contribute to the overview in the WinCC project data. A concept for picture selection and picture navigation should be planned prior to the beginning of the project. This is described in chapter "Creating the graphic user interface (Page 77)".

See also

- WinCC Information System > Working with WinCC > Working with Projects > Creating and Editing a Project > Preparation to Create a Project

5.1.2 Multi-user engineering

The configuration of comprehensive WinCC projects can be performed in parallel by different computers and by different users, whereby the users edit different resources. Release for multi-user engineering is activated in a property on the WinCC server. A resource dialog provides an overview of which resource is in process on which computer.

In contrast to remote configuration via a configuration client, with multiuser engineering the configuration clients do not have to be entered in the computer list.

See also

- WinCC Information System > Working with WinCC > Working with Projects > Creating and Editing a project > How to Use Multiuser Engineering

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), 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.

For the dynamization, 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.

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 to an fpt file. This faceplate type is inserted as a faceplate instance in the process pictures. Subsequent changes to a faceplate type are automatically updated in all instances.

The faceplate properties are specified individually in a configuration dialog. For dynamization, the object properties are connected to interface tags or structure elements. When they are instantiated, the faceplates are connected to the WinCC tag management.

The ftp files are stored in the WinCC project data in GraCS folder. The files can be transferred to a different WinCC project in the same folder using the Windows copy function.

See also

- WinCC Information System > Working with WinCC > Creating Process Pictures > Working with Faceplate Types

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. A change to the user object properties "Display" and "Operator control enable" can be passed on to all inner objects.

Structure tags are recommended to make user objects dynamic. Dynamic wizards integrated in WinCC Explorer support the connection and rewiring of the structure tags.

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

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

See also

- WinCC Information System > Working with WinCC > Creating Process Pictures > Working with Objects > Working with Combined Objects > Working with User Objects.

5.2.3 Picture 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. For dynamization, when a picture is called the tag prefix of a structure tag is transferred.

See also

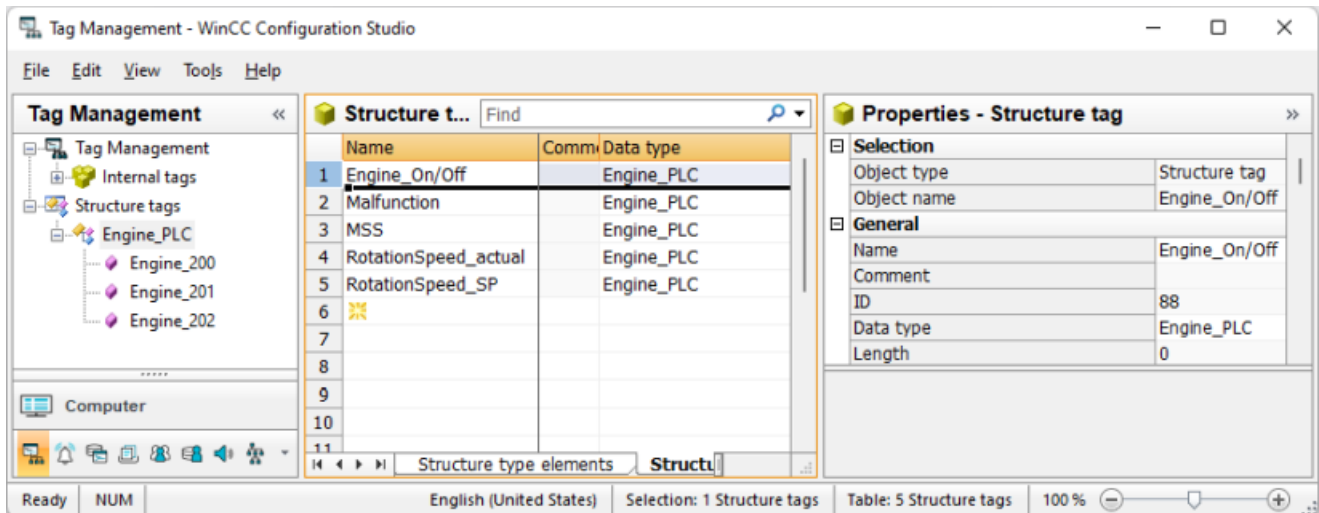
- WinCC Information System > Working with WinCC > Creating Process Pictures > Working with Objects > Working with Smart Objects > How to Insert a Picture Window

5.2.4 Structure tag

Structure tags are used to dynamize picture windows, user objects and faceplate types. A structure type is defined in WinCC for a process unit, for example, a motor, and contains all tag types for the motor as structure elements.

Tag structures that have already been defined as PLC data type (UDT) in the S7-1500 automation system can be transferred to WinCC tag management as structure tags. Direct transfer is possible with an existing online connection between WinCC Runtime and the AS. An import function is available as an alternative.

The example shows a simplified form.



5.2.5 Graphics Designer libraries

In the Graphics Designer, a differentiation is made between a library and an SVG (Scalable Vector Graphics) library. A large number of preconfigured graphical objects are available in the global library and the global SVG 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. The graphic symbols of the type SVG have dynamizable properties.

To store user-defined objects, object groups or user objects, the **project library** can be used. These objects that were developed, tested and qualified individually, are then inserted in the project library and are available as a project standard for multiple use in process pictures for the current project.

The project library is stored in the WinCC project in the "\library" directory. To allow its use in other projects, the contents of this directory is copied to the corresponding folder of the destination project.

Dynamized SVG graphics are inserted via drag-and-drop into a "Project SVG library" created for a specific project. In the WinCC project, the SVG libraries are found in a subdirectory of the "\GraCS" folder. An export function is used to save the symbols to a zip file. The SVG graphics are either added from a selected folder or by importing from a previously exported zip file of the project SVG library.

Note

To keep the effort for verification of process pictures to a minimum, it is advisable to use standard symbols whenever possible.

See also

- WinCC Information System > Working with WinCC > Creating Process Pictures > Working with Objects > Working with the Libraries
- Application example "Basic Process Library", Online Support under entry ID 109749508 (<https://support.industry.siemens.com/cs/ww/en/view/109749508>)

5.2.6 Project functions in the form of scripts

C and VB scripts are user-specific written programs that belong to software category 5. This type of software is developed to meet customer-specific demands not covered by standard functions.

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.

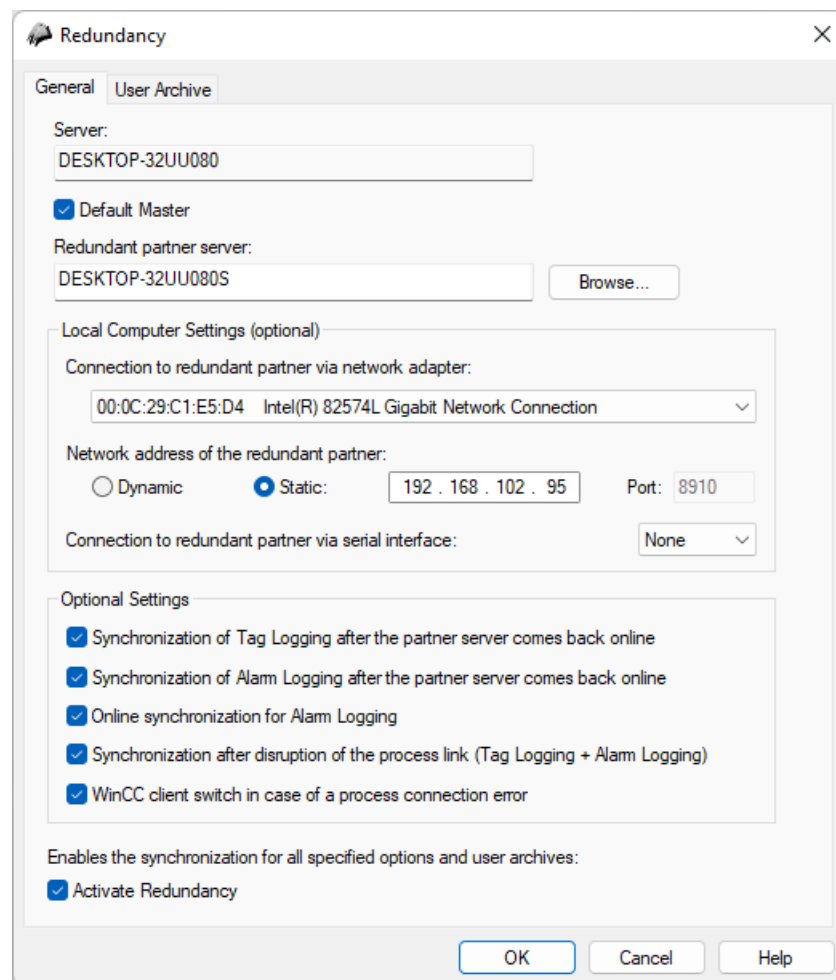
In general with such customized scripts, the calculation should take into account an increased amount of work for validation in the form of detailed functional and interface descriptions as well as documented tests.

See also

- WinCC Information System > Working with WinCC > VBS for Creating Procedures and Actions
- WinCC Information System > Working with WinCC > ANSI-C for Creating Functions and Actions
- WinCC Information System > Working with WinCC > Dynamize Process Pictures
- WinCC Information System > Smart Tools > WinCC Cross Reference Assistant
- Software categorization, see chapter "Software categorization according to GAMP Guide (Page 115)"

5.3 Configuring redundancy

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



The settings for the connection to the redundant partner server are configured here.

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

5.4 Time synchronization

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

See also

- WinCC Information System > Configurations > Redundant Systems

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 again operating.

See also

- PM-QUALITY on the Internet (<https://www.siemens.com/process-management>)

5.4 Time synchronization

Time synchronization is an important feature in automated systems in the GMP environment. In the case of interaction between multiple automation (AS) and/or operator stations (WinCC clients), it is important that messages, alarms, trends and Audit Trail data are recorded with synchronized time stamps.

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

The time stamps are generated in UTC and stored in the archives of the WinCC server. During plant operation, all the process data stored in the archive (messages and trends) are displayed converted from UTC to the time zone set in the Windows system (taking the daylight-saving/standard time setting into account).

The activation of the time synchronization in SIMATIC WinCC means that an active time master takes over the synchronization of all WinCC servers, WinCC clients, automation systems and, if present, the engineering station. To ensure synchronized time, all the stations in the system must be synchronized so that messages can be processed in the correct chronological order throughout the plant (archiving of trends, messages, redundancy synchronization of servers).

Note

The activation of time synchronization is necessary in plants in which GMP is mandatory.

5.4.1 Time synchronization concepts

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 functional specification.

When using the WinCC option "Basic Process Control", which is included in the scope of delivery of the SIMATIC WinCC system software, time synchronization can be configured in the Time Synchronization editor. Time synchronization via the terminal bus is preferable to time synchronization via the plant bus.

Time synchronization in a Windows workgroup

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

Time 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

- WinCC Information System > Options > Options for Process Control > Time Synchronization
- FAQ "Settings for time synchronization", Online Support under entry ID 16622902 (<https://support.industry.siemens.com/cs/ww/en/view/16622902>)

5.4.2 Time stamping

The specification of a plant subject to GMP must describe the way in which time stamping is to be performed. The accuracy necessary for message and process value acquisition must be checked in detail. The methods of time stamping mentioned below can be used alongside each other.

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 S7-300/400/1500.

With the bit messaging, the message is detected based on 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 are lost if they are shorter than the acquisition cycle.

5.4 Time synchronization

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 messaging.

Note

The bit messaging and limit value monitoring can be used with a single-station system in WinCC. In redundant systems or WinCC systems with several operator stations, chronological signaling is used for coordinated acknowledgment and transmission. With this message procedure, the controller sends a frame with the data of the message. The time stamp is assigned directly when the message occurs in the controller.

The Program_Alarm instruction in the SIMATIC S7-1500 or the SFCs/SFBs Alarm, Alarm_S/SQ, Alarm_D/DQ, Alarm_8/8P in the SIMATIC S7-300/400 are used for chronological signaling.

See also

- WinCC Communication to S7-1500, S7-1200 and ET 200SP, Online Support under entry ID 101908495 (<https://support.industry.siemens.com/cs/ww/en/view/101908495>)
- "How do you implement chronological messaging with S7-400 CPUs and WinCC?", Online Support under entry ID 23730697 (<https://support.industry.siemens.com/cs/ww/en/view/23730697>)
- WinCC Information System > Working with WinCC > Setting up a message system > Configuring the message system > Working with AS Messages

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 configured acquisition cycle.

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. This also applies to process values which are to be acquired in a cycle smaller than 500 ms.

See also

- WinCC Information System > Working with WinCC > Archiving Process Values > Basics of Archiving Process Values > Process Values and Tags > Structure of a Frame with Raw Data Tags
- Exchange of large data volumes between S7-300/400/1500 control system and WinCC, Online Support under entry ID 37873547 (<https://support.industry.siemens.com/cs/ww/en/view/37873547>)
- WinCC Information System > chapter 4.11.5.2 "Data exchange with the S7 function block AR_SEND"

5.5 Configuration management

The configuration of a computer system consists of various hardware and software components that may vary in complexity and range from commercially available standard components to specially customized user components. A clear and complete overview of the current system configuration must always be available. 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. These are defined and documented with designation, version number, etc. If customer-specific hardware is used, more work is required; see chapter "Selecting the hardware components (Page 24)" for more information.

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 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 of 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

The following chapter "Versioning application software (Page 71)" includes examples of how individual software elements can be versioned. Always consult the plant operator to agree upon a procedure for making changes to a plant in ongoing operation. (see chapter "Operational change control (Page 128)")

See also

- GAMP 5 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 reflected by incrementing 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.

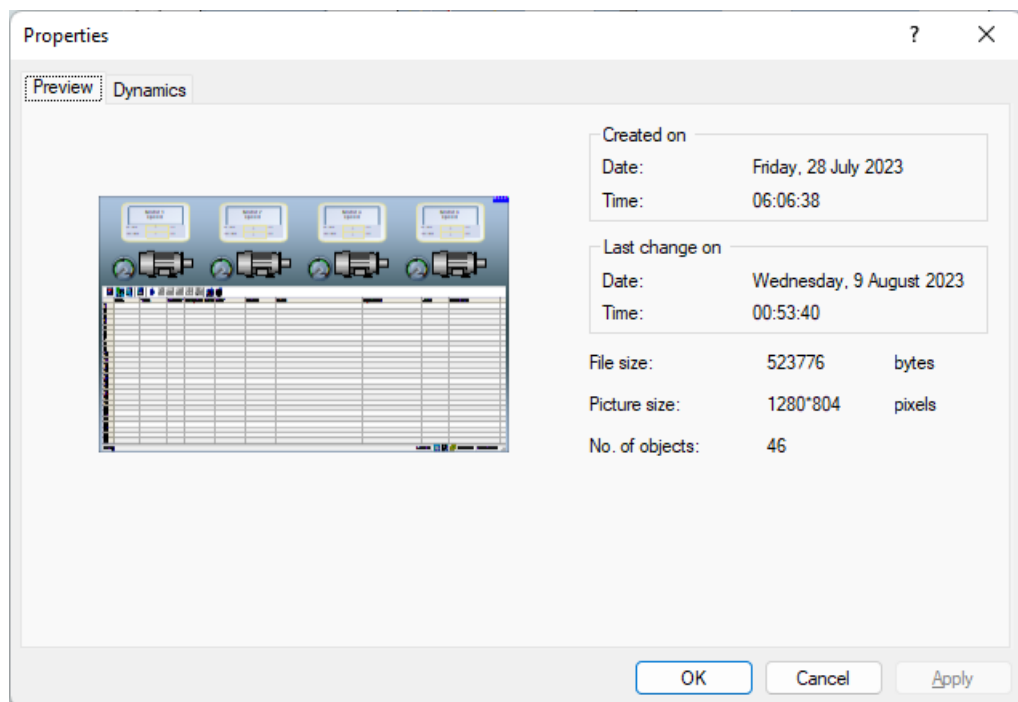
The following data is specified for the versioning of the application software:

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

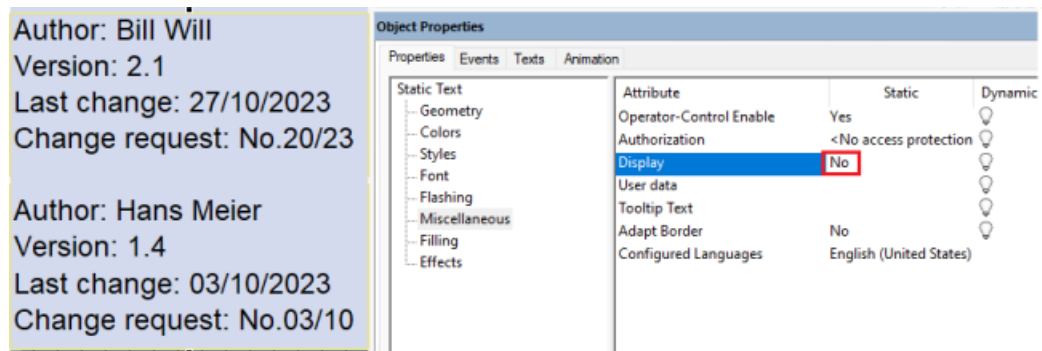
The following chapters show various examples of software element versioning.

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.



Note

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

5.6.2 Versioning VB / C scripts

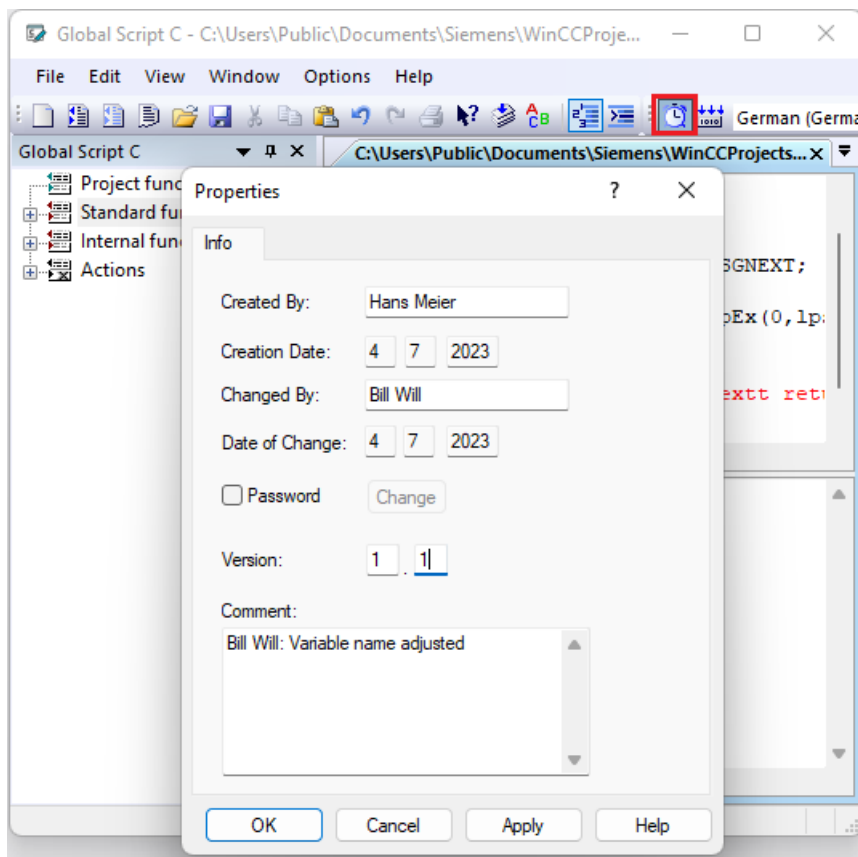
VB or C scripts are created to access tags and graphic picture objects during operation and to trigger actions that are not dependent on pictures.

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 fields in the **Properties > Info** 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:

```
E:\WinCCProjects\Demo_FCT_V75\Demo_FCT_V75.mcp : my_funktion.fct x
//-----
//
//Function: my_Function
//
//History:
//03/04/2015      Hans Meier   File has been created
//03/05/2015      Hans Meier   Fault xxx has been cleared
//06/27/2019      Bill Will    Tag interface has been modified
//
//-----
void my_Function()
{
  GetTagDWord("Bottles_CurrentValue");    //Return-Type: DWORD
}
```

Example of recording the history in a VB script:

```
Demo_FCT_V75.mcp: (Project Module) MyProcedure.bmo x
'-----
' Function: MyProcedure
'
'Historie:
'03/04/2015      Hans Meier   Script has been created
'03/05/2015      Hans Meier   Fault xxx has been cleared
'04/20/2015      Ben Will     Function yyy has been added
'06/27/2019      Bill Will    Tag interface has been modified
'-----
Sub MyProcedure
  Dim var1
```

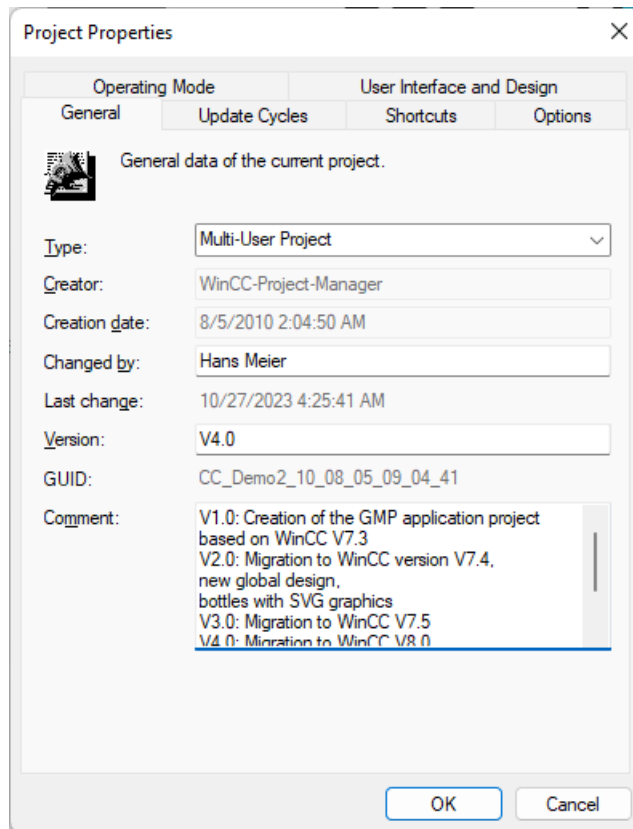
5.6.3 Versioning reports

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.

SysTime	Version: 2.1	SysPage
SysLayoutName	SysProjectName	

5.6.4 Versioning of the entire WinCC project

In WinCC Explorer the Project Properties dialog is opened at the top node. The *General* tab offers fields for entering the data **Creator**, **Version** and **Comment**. All further data is generated automatically by WinCC. Automatic versioning is not supported.



A history of the version changes, for example, can be maintained in the comment field. This serves as supplementary information if no additional software for project versioning is used.

See also

- Chapter "Versioning (Page 119)"

Creating Application Software

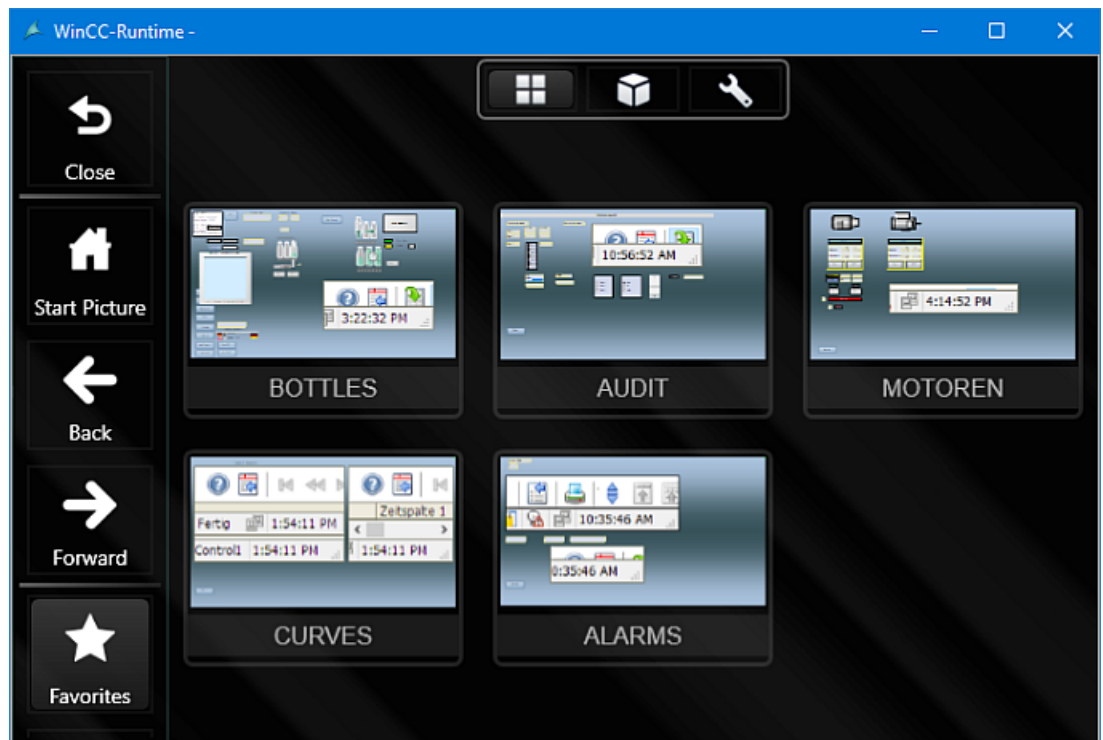
In a full automation solution, SIMATIC WinCC handles the operator input, monitoring and data archiving functions. The interface to the automation level is over powerful process links, see also chapter "Interfaces to SIMATIC WinCC (Page 108)".

This chapter explains tips and recommendations for the configuration of SIMATIC WinCC in a GMP environment. The configuration of the automation level is not described in this manual.

6.1 Creating the graphic user interface

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.

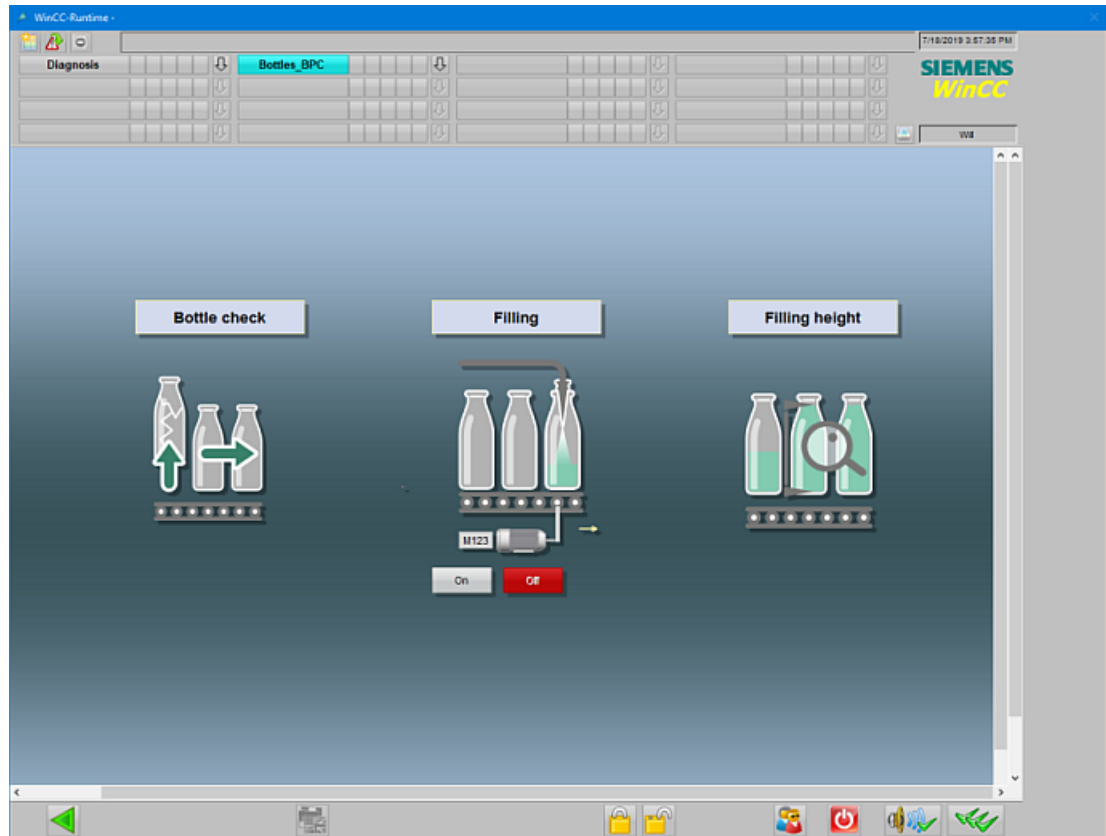
To visualize the plant or process, process pictures are created to allow operator control and monitoring according to the specified requirements. Possible elements are described in chapter "Object-oriented configuration (Page 64)".



In processes with several process pictures, it is advisable to define a system for picture selection and/or picture navigation. The *Menus and Toolbars* editor offers flexible design options. Picture selection via the runtime system dialogs with selected favorite pictures is particularly suitable for machine-oriented touch operation.

6.1.1 Standardized user interface

A standardized user interface in which the user-specific process pictures are only embedded is offered by SIMATIC WinCC with the Basic Process Control module. This module includes the *OS Project Editor*, *Picture Tree Manager*, *Time Synchronization*, *Horn* and *Lifeline Monitoring* editors.



The *OS Project Editor* is used to automatically create 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.

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.

See also

- Chapter "Time synchronization concepts (Page 69)"

6.1.2 Creating process pictures in the Graphics Designer

The Graphics Designer is a combination of a graphics program and a tool for representing processes. Based on the Windows standard, the Graphics Designer provides functions for the creation and dynamic modification of process pictures.

A number of essential elements for configuration are introduced in chapter "Object-oriented configuration (Page 64)".

Configuration of I/O fields

For display in the process picture, tags can be directly moved to the process picture in a drag-and-drop operation. For this purpose the Graphics Designer has a "Tag" window for selecting tags. After embedding with drag-and-drop, the process connection is already configured for the I/O field. Additional object settings can be made.

Output window

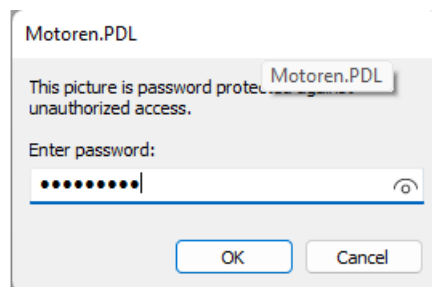
The output window in the Graphics Designer shows information, warnings and errors (e.g. on script functions on objects) after saving the process picture. Double-clicking the error entry selects the object in question in the picture.

Multilingual user interface

The user interface can be configured in several languages. Text and text layout in multiple languages can be entered directly for the individual objects, e.g., static text. Alternatively, when the configuration has been completed the texts are exported from the Text Distributor editor and imported again after the translation.

6.1.3 Password protection for process pictures

For know-how protection of the configuration, in particular for the protection of integrated VBA scripts, each process picture, and each faceplate type can be protected with a password. For opening in the Graphics Designer, the defined password must be entered.



6.2 Creating operator input messages

For plants operated in a GMP environment, international regulations such as regulation 21 CFR Part 11 in the USA or the EU GMP Guide Annex 11 require that operator input to the process that affects data relevant to GMP can be traced.

GMP-relevant operator inputs which are made using different operating elements such as, for example, IO fields, check box, radio box or buttons must therefore be configured in the WinCC Graphics Designer in such a way that an operator input alarm is generated. This operator input message is recorded in WinCC Alarm Logging with the time stamp, user ID, old value and new value.

Optionally, a mandatory comment for operation can be configured as well.

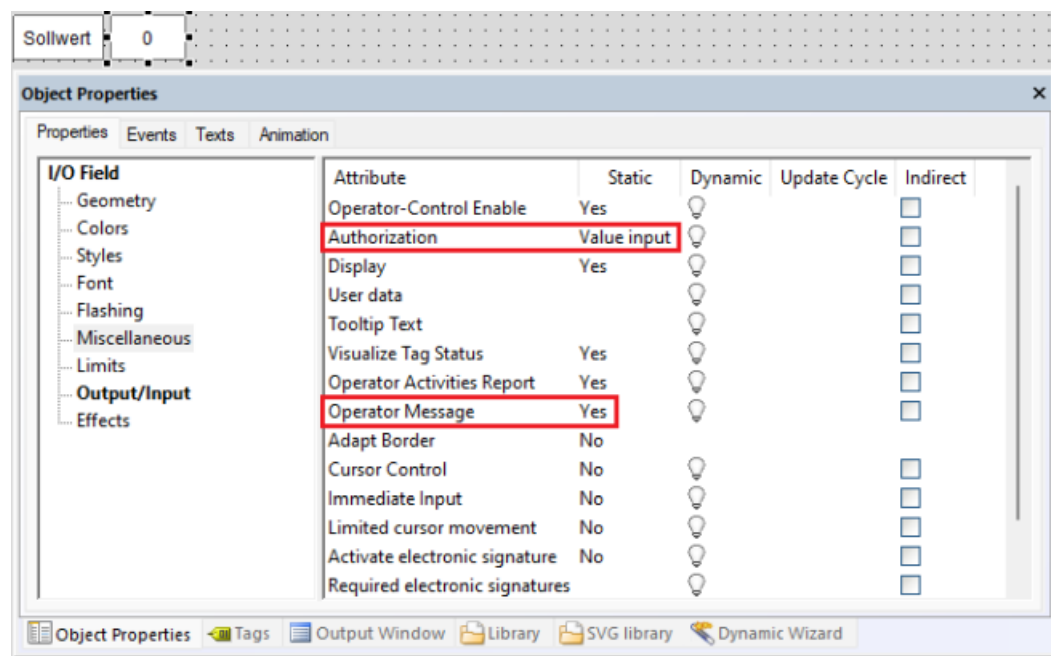
When the WinCC/Audit option is used, the operation messages including their comments are also transferred into the Audit database.

See also

- WinCC Information System > Working with WinCC > Setting Up a Message System
- System manual "WinCC/Audit", Online Support under entry ID 109818158 (<https://support.industry.siemens.com/cs/ww/en/view/109818158>)

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 permission is also set in the object properties for the I/O field using the "Authorization" attribute. This ensures that only a logged-on user with the appropriate authorization can perform a value change.



The generation of the standard operating message can be activated in this way for all objects that have the operator message property.

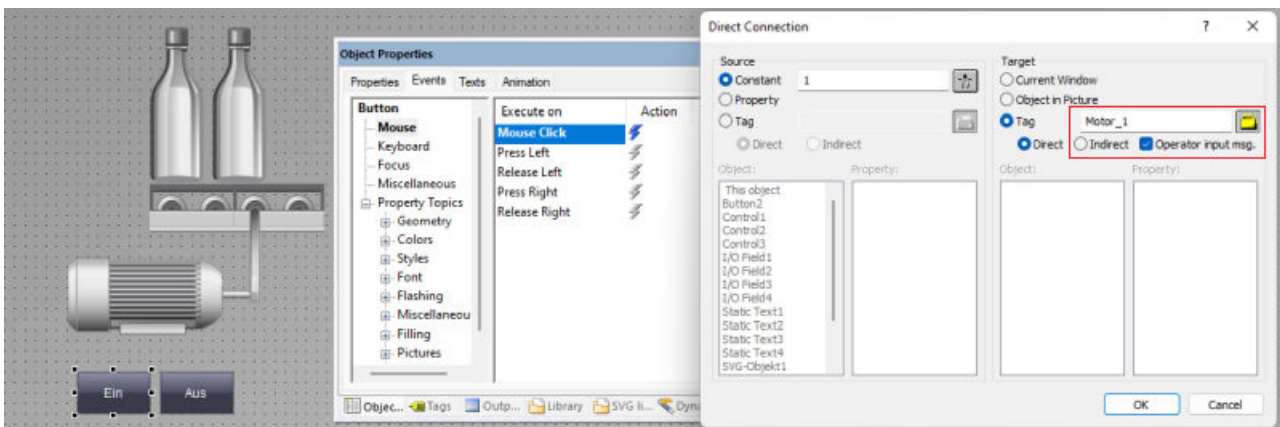
Operator input messages in conjunction with faceplate types

For input fields that are integrated in faceplate types, operation messages and/or operation logs are activated in the same way as described above under input/output field. The authorization for the operation of the input field should also be configured so that only authorized users can make changes. The operator message shows the value change in the connected structure or interface tag.

The same procedure also applies to other objects that have the operator message property.

Button

To operate buttons, the standard operator input message is only generated if a direct connection to a tag has been configured. For this purpose the "Operator input msg." check box is selected in the configuration dialog. It is 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 fields and buttons are not adequate, a user-specific operator input message can be generated using VB or C scripts. A corresponding example in the form of a project function as a C script is available for download in the Online Support under entry ID 24325381 (<https://support.industry.siemens.com/cs/ww/en/view/24325381>).

In VB script, the HMIRuntime.Alarms object is used to create a user-specific operator input message. User-defined operator input messages generated on the basis of scripts can also be supplemented with comments.

See also:

- WinCC Information System > Working with WinCC > VBS for Creating Procedures and Actions > VBS Reference > Objects and Lists > Alarms Object
- WinCC Information System > Working with WinCC > ANSI-C for Creating Functions and Actions > ANSI-C Function Descriptions > Standard Functions > Alarm > GCreateMyOperationMsg

Operator input message in the picture window

In a picture window, the generation of the operator input message for the individual GMP-relevant operator control elements is enabled in the "Operator Input Message" property. A user-specific operator input message can be generated for buttons as an alternative to direct connection (standard operator input message). The configuration works in all instances. When the screen window is called in runtime, the appropriate operator input messages are generated.

Operator input message in faceplate type

In a faceplate type, the generation of the operator input message is enabled for GMP-relevant entries, e.g., in I/O fields. The operator message for buttons in faceplate types cannot be instantiated. Therefore, the generation of the operation messages for buttons at each individual instance are either configured in the direct connection to a tag (standard operation message) or via VB script (user-specific operation message).

Note

In the GMP environment, picture windows are preferred for the operation of units such as drives, valves, etc. Faceplate types are suitable for the specification and display of values.

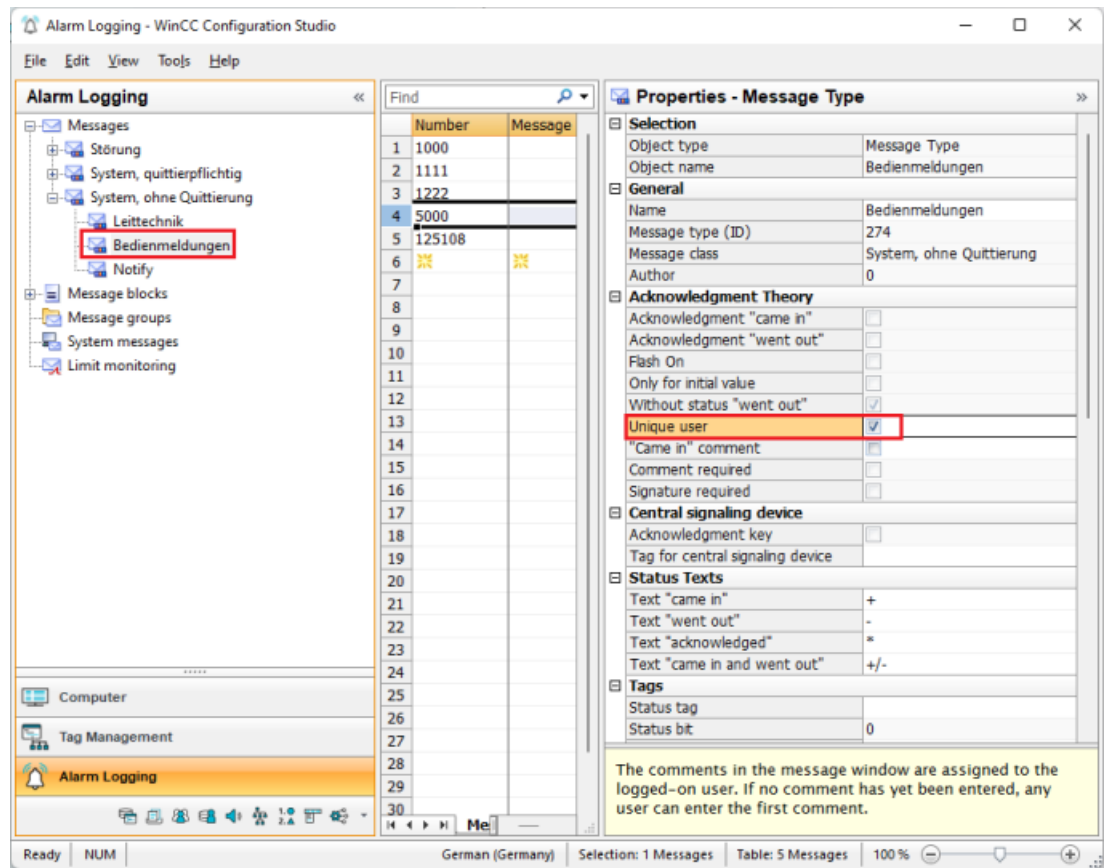
See also

- Comparison of picture window and faceplate technologies in WinCC Professional / WinCC V7.5, Online Support under entry ID 109764584 (<https://support.industry.siemens.com/cs/ww/en/view/109764584>)

Operator activities report / operator activities comment

In Alarm Logging, the comment for the operator input message (operator activities report) is displayed by a button in a dialog. The comment cannot be modified later. However, further comments on the operation message can be added.

In addition, the "Unique user" property can be activated in the Alarm Logging for the various message classes. Therefore only the user who generates the operation message and who has entered the comment may add further comments on this message. The operator must be logged in to WinCC Runtime for this purpose.



Acknowledgment of messages as operator input message

Various operator actions (lock, release, hide, show, acknowledge) in the alarm view can be documented with an operator input message. For example, a system message is generated for the acknowledgment of a message. This system message receives the time stamp of the acknowledgment, the logged-on user, and a reference to the acknowledged message. A comment or a signature for acknowledging a message can also be configured.

- WinCC Information System > Working with WinCC > Setting Up a Message System > Configuring ... > Working with message types (chapter 3.8.4.4)

Acknowledgment of messages with mandatory comment

The traceability of message acknowledgments in GMP-relevant production plants is more transparent with the input of mandatory comments. A mandatory comment when a message is acknowledged can be configured in WinCC Alarm Logging. An operator input message with the entered comment is generated for the acknowledged message.

The mandatory comment can also be combined with a signature so that entry of a comment is required in the signature dialog. For this purpose, the operation message must be activated in both the AlarmControl properties and the Alarm Logging.

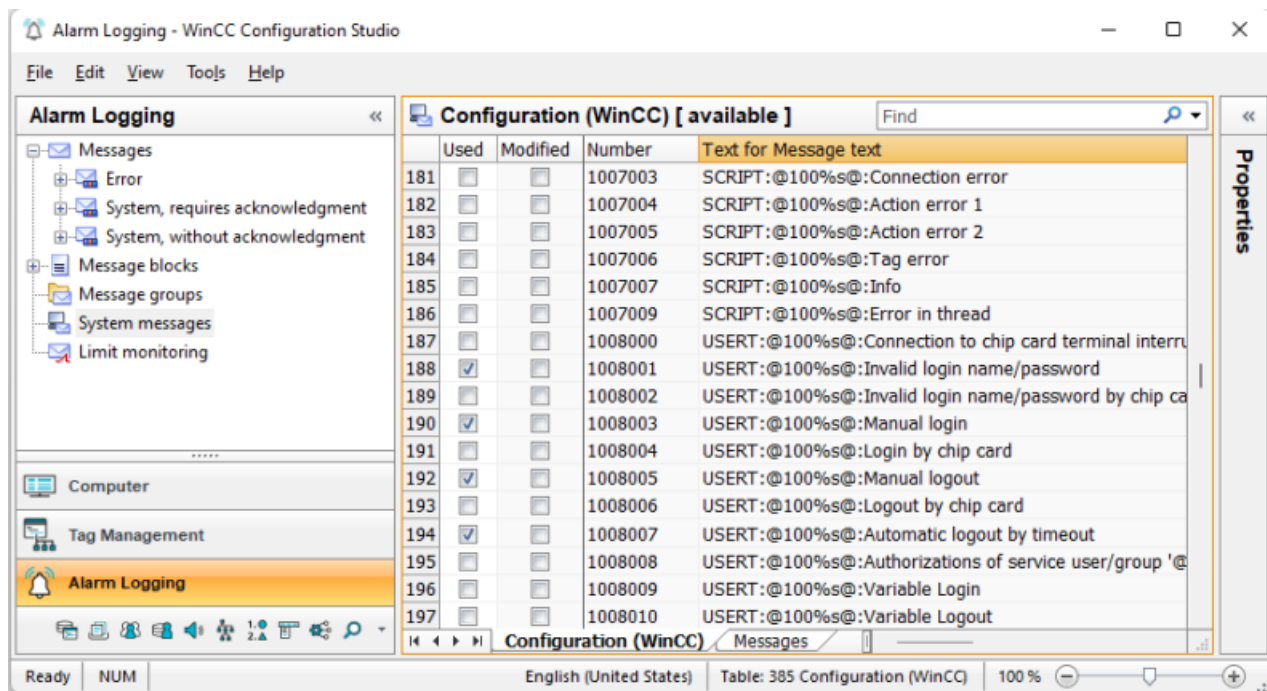
6.3 Audit trail and change control

6.3.1 Audit trail for operator actions

Operator input through input/output fields, buttons or through other objects can be configured in the WinCC Graphics Designer so that an operator input message is generated by the system. (For information on configuration see chapter "Creating operator input messages (Page 80)")

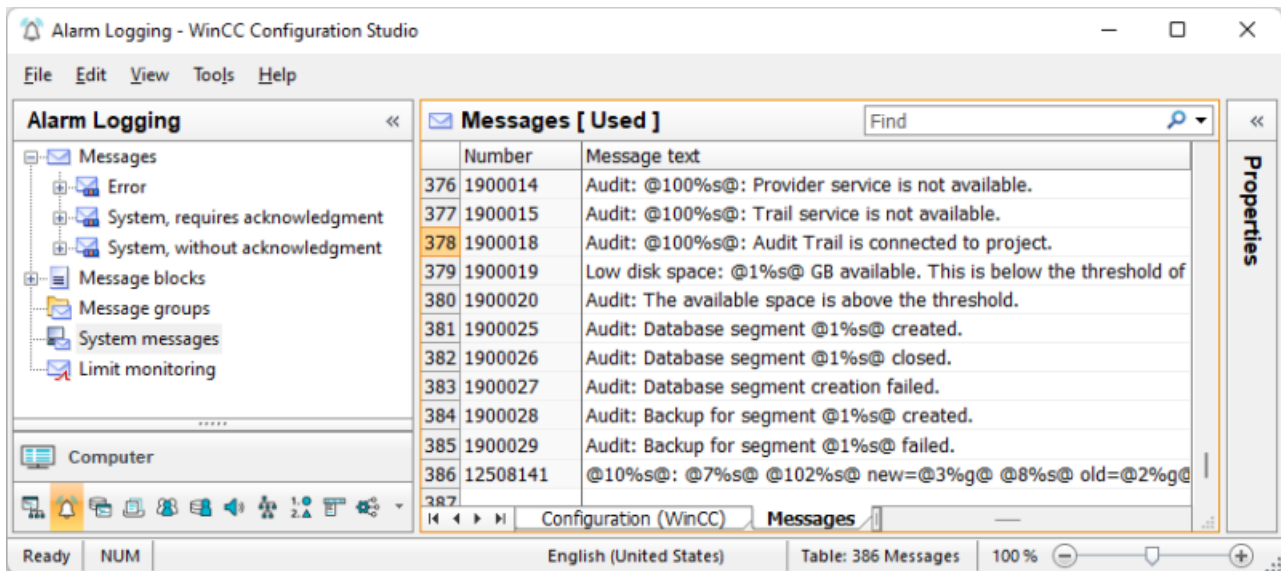
In addition to the operator message, login and logout processes can also be archived in WinCC Alarm Logging. WinCC provides a series of system messages which can be activated for recording in Alarm Logging, if required.

When the WinCC/Audit option is active, these messages are also entered in the Audit database.

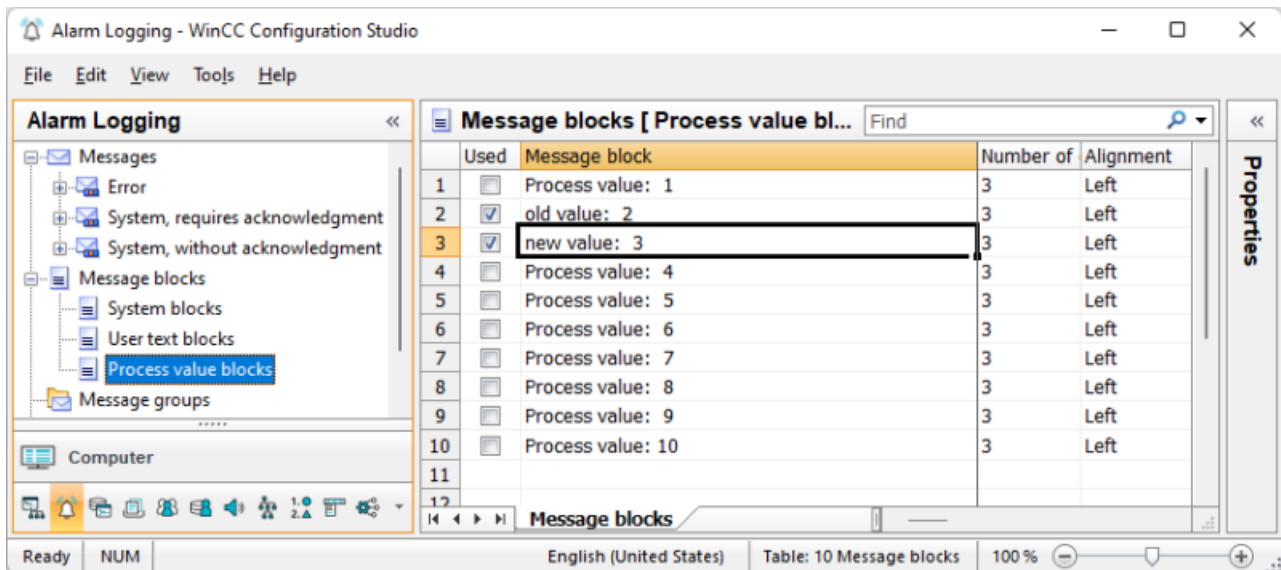


To record the logon/logoff processes via a Web client, the message numbers 1012400 and 1012401 are activated in addition.

The "Messages" table shows the "used" system messages. The operator input message with the message number 12508141 is automatically listed.

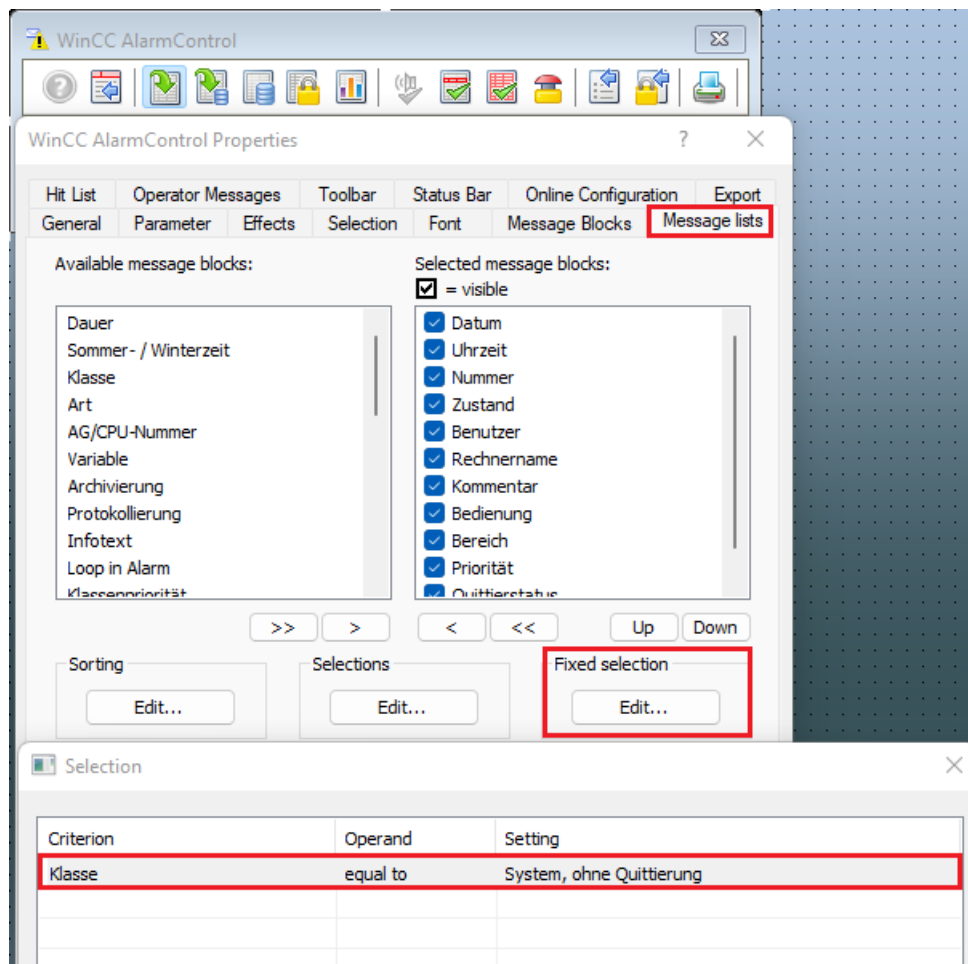


The operator input message is a standardized system message for which the system automatically enters the old value in process value 2 and the new value in process value 3. We therefore recommend that you rename process value blocks 2 and 3. The system messages cannot be configured.



The **WinCC AlarmControl** is dragged from the object palette into a screen for the display of the operation messages.

A double-click on the control opens the **Properties** dialog. A "fixed selection" is defined in the *Message lists* tab so that only operation messages are displayed in the AlarmControl. The criterion **Class** is selected in the configuration dialog and is **equated** to the setting **System, without acknowledgment**.



This means that only operator input messages, including user-specific operator input messages, as well as login/logout processes are displayed in the WinCC AlarmControl.

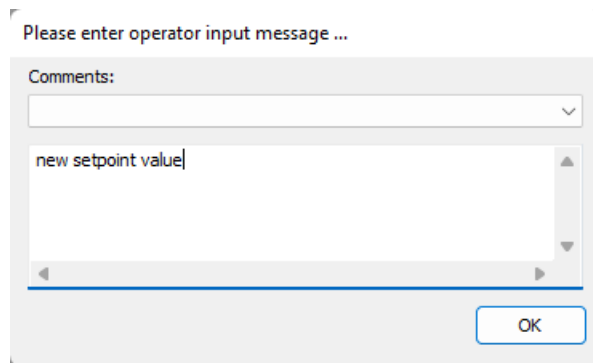
The audit trail is displayed in the process picture as follows:

	Date	Time	Number	User name	Comments	old value	new value	Message text
64	27/02/24	11:35:40	AI 12508141	admin_1		15	20	Value_1: admin_1 new=20 old=15
65	27/02/24	11:35:44	AI 12508141	admin_1		10	12	Value_2: admin_1 new=12 old=10
66	27/02/24	11:35:53	AI 12508141	admin_1		7	115	Value_3: admin_1 new=115 old=7
67	27/02/24	11:36:02	AI 12508141	admin_1		115	18	Value_3: admin_1 new=18 old=115
68	27/02/24	11:36:57	AI 12508141	admin_1		12	14.5	Value_2: admin_1 new=14.5 old=12
69	27/02/24	11:37:14	AI 12508141	admin_1		20	18	Value_1: admin_1 new=18 old=20

Ready Pending: 0 To acknowledge: 0 Hidden: 0 List: 71 11:45:23 AM

The symbol in the **Comment** column shows that a comment is available. This can be displayed with the button marked in the screenshot or by double-clicking the column for the selected message.

The WinCC/Audit option makes the WinCC AuditViewer Control available. If it is integrated into a screen, the entries from the Audit database can be called during runtime.



The comment cannot be modified later. However, further comments can be added. Apart from the user name of the logged-on operator, they also include the location and time stamp of the created comment. This applies to the automatically generated standard operation message with Operator Activities Report (message number 12504181) as well as to the user-specific operation messages generated via script.

See also

- Chapter "Creating operator input messages (Page 80)"
- System manual "WinCC/Audit", Online Support under entry ID 109818158 (<https://support.industry.siemens.com/cs/ww/en/view/109818158>)

6.3.2 Change control for the configuration and project engineering

Backup of the overall configuration

The WinCC configuration, as well as the project engineering (pictures, scripts, etc.), is backed up and archived together with the overall project. Changes are subject to the applicable change procedures and must be controlled.

Change control in the configuration

Like other changes, changes to the individual OS elements have to be controlled with the applicable change procedure. You are supported by the tools used for the documentation of the changes. Various system functions are available for this purpose.

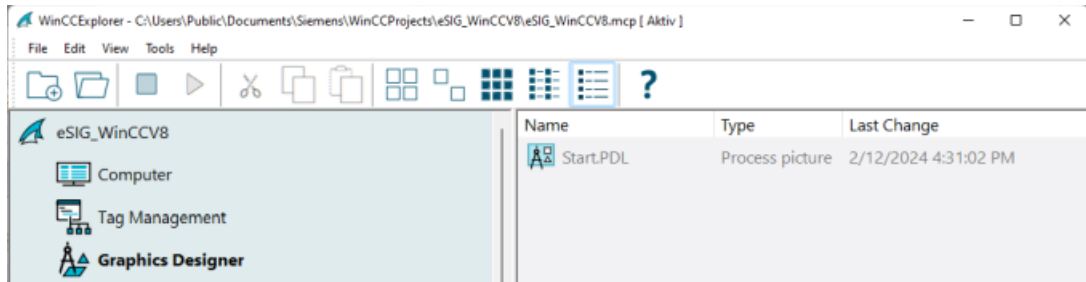
In addition to the user activities in WinCC Runtime, the WinCC/Audit option can also record WinCC configurations. Furthermore, Document Control enables the document management of WinCC screens, C and VBS functions, reports and user documents.

See also

- System manual "WinCC/Audit", chapter 3.6.3 "Working with Document Control and Project Versioning", Online Support under entry ID 109818158 (<https://support.industry.siemens.com/cs/ww/en/view/109818158>)

A simple way of controlling is to document the performed changes by means of screenshots and attach these to the change request.

Changed operating screens can also be identified by the date of change in WinCC Explorer. In addition, the operating screens can also be protected from modification via the WinCC Explorer with a password; see also chapter "Write protection (Page 121)".



6.4 Electronic signature

If electronic signatures are to be used in a computer system instead of handwritten signatures, certain legal regulations must be complied with, such as those contained in 21 CFR Part 11 of the U.S. Food and Drug Administration or also Annex 11 of the EU GMP Guide.

Other laws and regulations or the process owner define the actions for which signatures are required. The process owner is always the one who decides the actions for which signatures will be provided electronically.

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

Example of a simple electronic signature with a separate dialog

A setpoint is to be changed. When the I/O field is left, a screen window appears in which an authorized user signs electronically by entering a user name and password. Only then is the setpoint change carried out. The setpoint change as well as the signature provided are recorded in the Audit Trail.

The screen window for the electronic signature includes the actions to be performed, the authorized user group as well as the fields for authentication of the user. In addition, the entry of a comment can be configured as optional or mandatory.

Electronic Signature - Identity Verification

Operation: Change tag value:
-Tag name: Setpoint_Temperature
-Old value: +5,00
-New value: +7,00

User group: \OPERATOR

User name: User_1

Password: ●●●●●●

Comment:

OK Cancel

Example of a multiple electronic signature

A multiple electronic signature is possible in combination with the WinCC/Audit option. An action must be signed by several persons with different roles in this case. The signatures can be provided "immediately" or "retroactively". The "immediately" setting should be selected so that all signatures are requested before the action becomes effective.

[illegible]

A setpoint is to be changed. An immediate multiple electronic signature is configured for the operation. After leaving the IO fields, the window for selection of the authorization group appears. The authorized user can complete the electronic signature of the selected authorization group. Another user must then provide the electronic signature for the other authorization group.

The figure below illustrates the associated messages of the multiple signature in the WinCC AlarmControl.

	Date	Time	Number	User name	Comments	Message text
56	23/08/23	12:01:44 PM	1900000	USER_1\OPERATOR		ESIG: Electronic signature of user [ID:12] USER_1 accepted.
57	23/08/23	12:01:52 PM	1900000	ADMIN_1\ADMINISTRATOR-GROUP		ESIG: Electronic signature of user [ID:11] ADMIN_1 accepted.
58	23/08/23	12:02:01 PM	12508141			Setpoint_Temperature: new=7 old=5

Ready Pending: 0 To acknowledge: 0 Hidden: 0 List: 58 12:04:22 PM

See also

- Chapter "Creating operator input messages (Page 80)"
- Chapter "Audit trail for operator actions (Page 84)"
- System manual "WinCC/Audit", Online Support under entry ID 109818158 (<https://support.industry.siemens.com/cs/ww/en/view/109818158>)

6.5 Recording and archiving data electronically

It is very important to provide consistent quality evidence 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, e.g.:

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

6.5.1 Determining 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 the data to be archived coming from different sources: process values, messages, batch data, reports, audit trails, log files, etc.
- Definition of the relevant recording cycles
- Specification of the period of storage online and offline
- Definition of the archiving cycle for transfer to external storage

This data is then stored in various archives:

- Process value archive "Tag Logging fast", archiving of process values <1 min
- Process value archive "Tag Logging slow", archiving of process values >1 min
- Message archive "Alarm Logging"

- PM-QUALITY database
- PM-CONTROL database
- PM-SERVER database for evaluation and analysis in PM-ANALYZE

On top of this, in other parts of the system, additional actions are monitored and recorded in log files or databases:

- WinCC reports
- SIMATIC Logon database "EventLog.mdb"
- Event Viewer under Windows Computer Management (logon/logoff activities, account management, permission 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 Setup of process value and message archives

Process value archive

A process value archive is used to save process values (analog and binary values) in a database in the form of a short-term archive.

The configuration is carried out in the "Tag Logging" editor, the following steps are required:

- Creating the required process value archives and selecting the tags that are to be recorded.
- Configuring the properties for each process value archive, such as archive size, storage location, signing activated, etc.

The archived process values are generally stored in compressed form in the archives. The "Signing activated" property generates a checksum when the archive segment is swapped out from the Microsoft SQL Server. For a later view of the data, swapped-out archive segments can be reconnected to the WinCC Controls. At the same time, the checksum is verified. A message signals whether a swapped-out archive was manipulated.

If a subsequent change or a new input of process values is to be possible, this can be implemented via the WinCC OnlineTableControl with corresponding operator authorization and operator activities report. Otherwise, this function must remain deactivated.

Message archive

All incoming messages are recorded in WinCC Alarm Logging. These are operating messages, operator input messages, alarm messages, system messages, control messages, limit monitoring, etc. The division into different message classes and message types determines the display and the acknowledgment requirement of the messages.

The settings for the messages, the archive size, and the swapping-out behavior are defined in the "Alarm Logging" editor in the Configuration Studio. Just like a process value archive, the message archive also has the "Signing Active" property.

6.5.3 Setting up user archives

The option "WinCC/User Archives" can be used for managing database tables with several data records, e.g. for simple machine data or small recipes. WinCC UserArchiveControl offers an overview of the data records created.

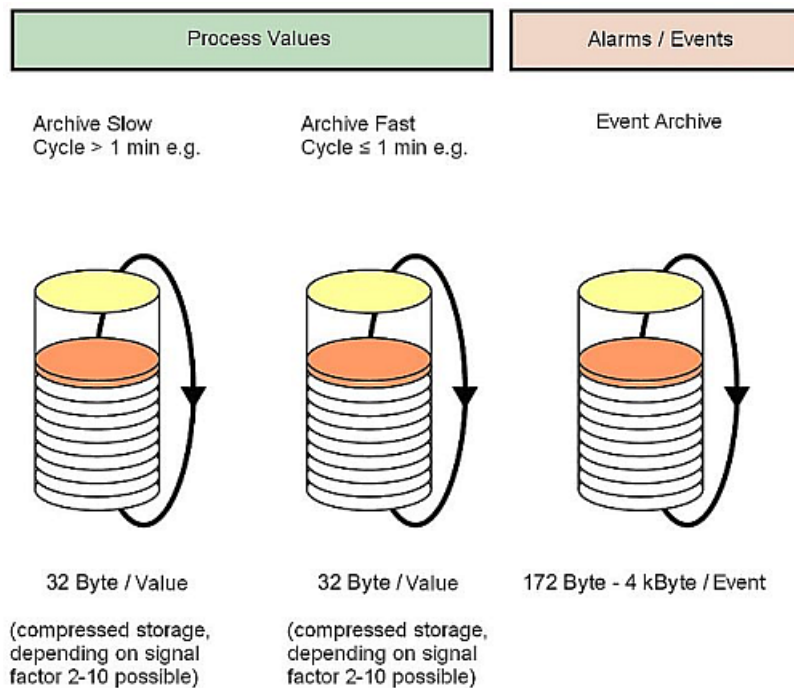
To comply with the GMP requirements related to the audit trail for changing critical parameter data (recipe data/machine data), such data fields are connected to I/O fields in a WinCC picture. The activated property "Operator input message at I/O field" triggers an operator input message when a value is entered.

See also

- Chapter "Creating operator input messages (Page 80)"
- WinCC Information System > Options > User Archives

6.5.4 Recording and archiving

Archiving in WinCC involves two steps. First, messages (Alarm Logging) and process values (Tag Logging Fast and Slow) are recorded as sequential archives in individual segments.



These short-term archives can be transferred to a long-term archive using a number of different solutions and can then be stored for a time period specified by the customer.

The size of the Tag Logging database is determined by the number of process value archives and the process tags contained there. The size of a process value archive depends on the smallest acquisition cycle for the process tags.

It is recommended to only back up values of process tags with the same acquisition cycles (e.g. 500 ms, 1 s, etc.) in a process value archive. A separate process value archive should be created for each acquisition cycle required.

Handling of the database in the WinCC/Audit option is described in the respective system manual, including backup and restoring.

See also:

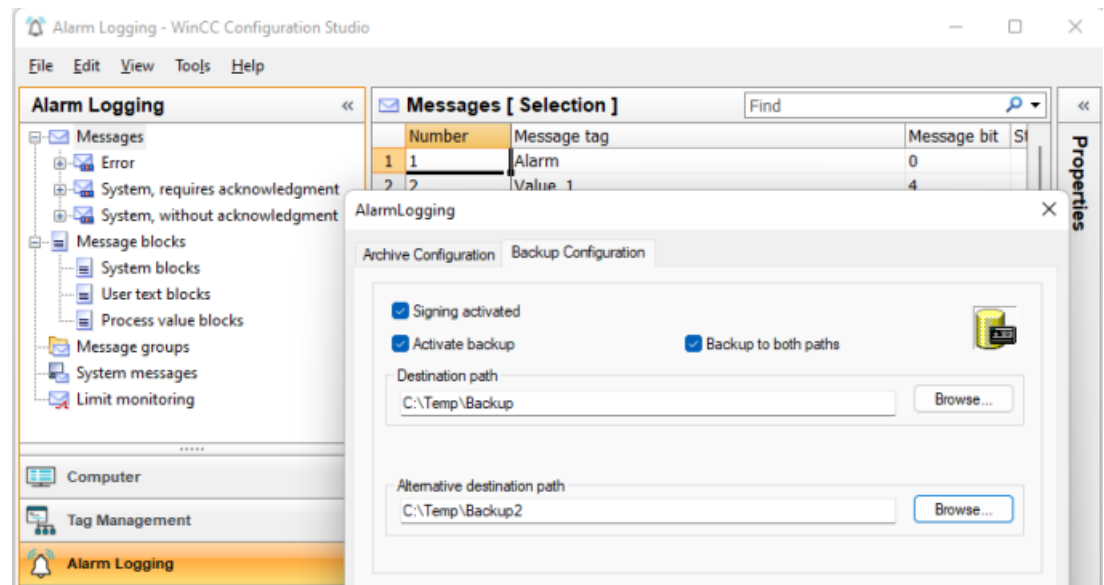
- WinCC Information System > Calculation of Memory Requirements
- System manual "WinCC/Audit" chapter 3.7, Online Support under entry ID 109818158 (<https://support.industry.siemens.com/cs/ww/en/view/109818158>)

6.5.5 Long-term archiving

The property "Relevant long term" is activated by default for the process tags. This is a requirement for the transfer of the recorded process values to the long-term archive or Process Historian. The messages recorded in WinCC Alarm Logging are always completely swapped out.

Long-term archiving with SIMATIC WinCC

For the long-term archiving of the process values (TagLogging Fast and TagLogging Slow) as well as the messages, backup and signing (checksum) are activated for each archive type and at least one target path is specified for the export.



To prevent losses due to failure of the long-term archive, an alternative second destination path can be specified.

Long-term archiving with the SIMATIC Process Historian

The WinCC option SIMATIC Process Historian archives process values and messages from one or more operating systems of the type WinCC, WinCC RT Professional and PCS 7 in a central database. The number of connected systems, including redundant systems, is not limited. The messages saved in WinCC archives are fully transferred to the Process Historian. Only those archive tags are taken over for which the "Relevant long term" property is activated. After installation of the Process Historian option, activation can be performed in the "Runtime" editor. For more information, see the following links.

See also

- System manual "Process Historian", Online Support under entry ID 109825371 (<https://support.industry.siemens.com/cs/ww/en/view/109825371>)
- Trend Viewer for the SIMATIC Process Historian 2014, Online Support under entry ID 109756715 (<https://support.industry.siemens.com/cs/ww/en/view/109756715>)
- Installation, operation and maintenance of Process Historian and of the Information Server in a PCS 7 environment, Online Support under entry ID 66579062 (<https://support.industry.siemens.com/cs/ww/en/view/66579062>)

Batch-based long-term archiving with PM-QUALITY

In PM-QUALITY, the acquired batch data can be exported manually or automatically in database, HTML, PDF or XML format. The acquisition of the data is described in chapter "Batch-based reporting with PM-QUALITY (Page 96)".

Only finalized and released batches can be archived (exported). After the automatic export, the batch is set to the status "finalized" in PM-QUALITY. Changes/additions to the batch data are thus no longer possible.

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 conversion to PDF format with the help of additional tools.

See also

- Chapter "Batch-based long-term archiving with PM-QUALITY (Page 37)"
- PM-QUALITY on the Internet (<https://www.siemens.com/process-management>)

6.6 Reporting

Depending on the application, various possibilities are available for reporting.

The WinCC Report Designer is used for documentation of both the configuration data and the Runtime data.

The WinCC Premium Add-on PM-QUALITY is used for batch-based acquisition and reporting of batch data.

The Information Server can be used in combination with the Process Historian to report historical data; see chapter Long-term archiving (Page 93).

The Information Server can also access the database of the WinCC/Audit option directly and can create reports; see chapter 3.7.9 in the WinCC/Audit system manual for information on this.

See also:

- System manual "WinCC/Audit", Online Support under entry ID 109818158 (<https://support.industry.siemens.com/cs/ww/en/view/109818158>)

6.6.1 Reporting with the WinCC Report Designer

The Report Designer is integrated in the WinCC system software to allow documentation of the configuration data and the runtime data. For multi-lingual projects, the report is created in the currently set Runtime language.

Various standard layouts and print jobs are available in the Report Designer for the documentation of the **configuration data**.

The following **Runtime data** can be logged, for example:

Message sequence report	Chronological listing of all messages that have occurred
Message report	Messages of the current message list
Archive report	Messages from the messages archive, for example, Audit Trail based on operator input messages
Tag table	Tag contents from process value / compressed archives in table format
Tag trend / picture	Tag contents from process value / compressed archives in Trend type
User archives (User Archive)	Contents of the user archives in the form of a table
Hardcopy	Reproduction of screen contents
CSV tables / CSV trends	Output of files in CSV format in the form of tables or trends

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. A ready-to-use layout also exists for the data from WinCC/Audit.

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

- 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 output of the data is based on a selection of the WinCC archives. For example, the Audit Trail entries are displayed as follows in the report.

Audit Trail

	Date	Time	Num	User name	Message text	Old value	New value	
1	15/08/19	09:13:19 PM	1250	Will	Motor1: Will new=1	0	1	
2	15/08/19	09:13:25 PM	1250	Will	Motor1: Will new=0	1	0	
3	15/08/19	09:13:52 PM	1111	Will	Will, old value: 48, n	48	46	
4	15/08/19	09:14:16 PM	1250	Will	Var_CB: Will new=2	2	3	
5	15/08/19	09:14:20 PM	1250	Will	Var_RB: Will new=2	1	2	
6	15/08/19	09:14:24 PM	1250	Will	Var_SI: Will new=20	45	29	
7	15/08/19	09:14:43 PM	1250	Will	Motor1: Will new=0	0	0	
8	15/08/19	09:15:02 PM	1111	Will	Will, old value: 46, n	46	50	
9	15/08/19	09:15:12 PM	1250	Will	Var_RB: Will new=1	2	1	
10	15/08/19	09:15:16 PM	1250	Will	Var_CB: Will new=1	3	1	

See also

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

6.6.2 Batch-based reporting with PM-QUALITY

The WinCC Premium Add-on PM-QUALITY is used for batch-based archiving and reporting of batch data. 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, and the batch name can be configured. The data can be retrieved under this batch name.

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

The following figure shows an example for a batch report.

15/12/2023, 12:32
Product_2023_12_15_2

PMQ Sample Project



Product batch header data
Product batch: Product_2023_12_15_2
12/15/2023 12:19:42 PM - 12/15/2023 12:23:17 PM
Timezone: W. Europe Standard Time

QR - Code


Batch header data
Batch name: Product_2023_12_15_2_Mixer2_1
Batch state: Process state

Batch times
Batch start time: 12/15/2023 12:19:42 PM
Batch end time: 12/15/2023 12:21:30 PM
Batch running time: 0:01:48

Setpoint value:

Time	Flour	Salt	Water	Yeast
12/15/2023 12:20:33 PM	17.5	375.0	3.3	125.0

Actual value:

Time	Flour	Salt	Water	Yeast
12/15/2023 12:20:33 PM	17.6	382.500	3.4	130.0

Batch header data
Batch name: Product_2023_12_15_2_Oven_1
Batch state: Process state

Batch times
Batch start time: 12/15/2023 12:21:32 PM
Batch end time: 12/15/2023 12:22:19 PM
Batch running time: 0:00:47

Baking time:

Time	Passed time
12/15/2023 12:22:14 PM	26

Batch header data
Batch name: Product_2023_12_15_2_Packaging_1
Batch state: Process state

Batch times
Batch start time: 12/15/2023 12:22:20 PM
Batch end time: 12/15/2023 12:23:17 PM
Batch running time: 0:00:56

file:///C:/Users/siemens/AppData/Local/Temp/Product%20_2023_12_15_2.htm

1/3

The procedure for including audit trail entries (operator input messages) in a batch report is shown below based on an example. The data from the database of WinCC/Audit can be imported into PM-QUALITY.

The message blocks to be displayed in the batch report are selected in the properties for the separate message group 'Audit', for example. The message number for the operator input message as defined in the WinCC system is also entered in the message filter dialog. Message numbers of user-defined operator input messages are also added.

The **Audit message group** is displayed in the area for the existing objects in the Report Layout editor. The audit message group is moved to the right for display in a report layout using drag-and-drop.

An audit trail can appear as follows in a batch report:

Timestamp ↓	Number	Comment	User	OldValue	NewValue	Instance
7/8/2019 3:47:50 PM.719	12508141	Red adaption	Will	10.000000	12.300000	PMQ_ParamRed
7/8/2019 3:48:21 PM.635	12508141	Yellow reduction	Will	20.000000	18.400000	PMQ_ParamYellow
7/8/2019 3:48:43 PM.657	12508141	More Blue	Will	30.000000	32.500000	PMQ_ParamBlue

See also

- PM-QUALITY on the Internet (<https://www.siemens.com/process-management>)

6.7 Monitoring the system

SIMATIC WinCC offers various options for monitoring communication. System tags signal the connection status, performance tags are used to evaluate the connection performance. The SysDiagControl control displays detailed information specifically for the S7-1200/ S7-1500 communication channels, and the Channel Diagnostics application provides information about the current state of the individual connections to the automation level. Information on the computer workload, hard disk capacity, etc. can be called via the system information channel.

See also

- Diagnostic options in WinCC and PCS 7 OS, Online Support under entry ID 48698507 (<https://support.industry.siemens.com/cs/ww/en/view/48698507>)

6.7.1 Evaluation of performance tags

For every connection to an automation system, the system tags ConnectionState and ForceConnectionState are generated, which provide information about the connection status.

When creating a new WinCC project, various performance tags are generated for WinCC tag management (Data Manager) and WinCC tag logging, which reflect the time response of the WinCC server. In addition, connection-specific performance tags are generated that contain information about the time response of the connection.

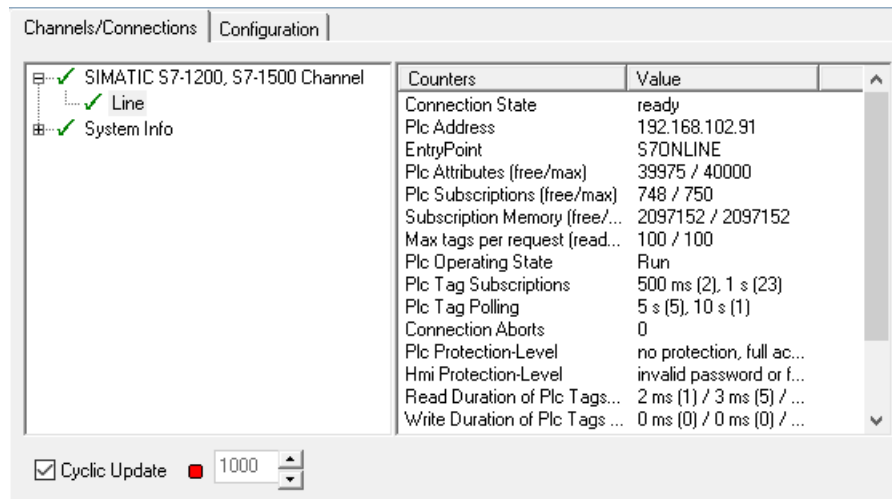
See also:

- WinCC Information System > Communication > Communication Diagnostics > Channel Diagnostics > Check connection with performance tags
- WinCC Information System > Working with WinCC > Making Settings in Runtime > System Diagnostics with Performance Tags

6.7.2 Diagnostics of communication connections

The WinCC application *Channel Diagnostics* provides an overview of the state of the communication connections to the lower-level controllers. The application can be integrated in a WinCC picture (for example a diagnostic picture) via the category *Siemens Automation > Channel Diagnostics* or as an ActiveX Control.

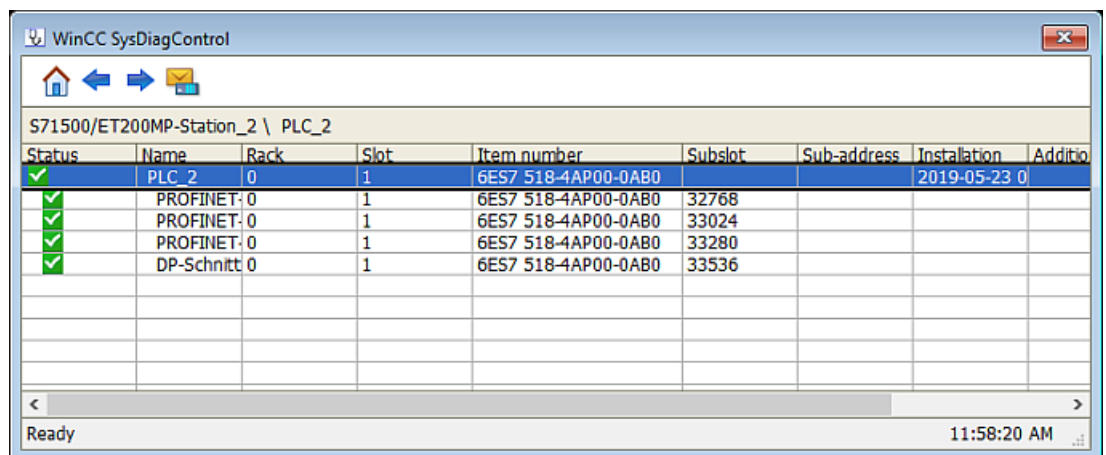
The status of the channels that support diagnostics is displayed in a window. A log file shows information about the start/end of the connection, version identification and error messages that are recorded automatically with time stamp. This represents evidence of the quality of the communication connections provided by the system.



6.7.3 Diagnostics for SIMATIC S7-1200 / S7-1500 channel

The SysDiagControl control is used to display errors and faults in S7-1500 / S7-1200 automation systems. All available connections with status information are listed in an overview. Additional details are displayed by double-clicking on a connection.

The diagnostic buffer of the automation system can be read out and displayed via a button.



See also:

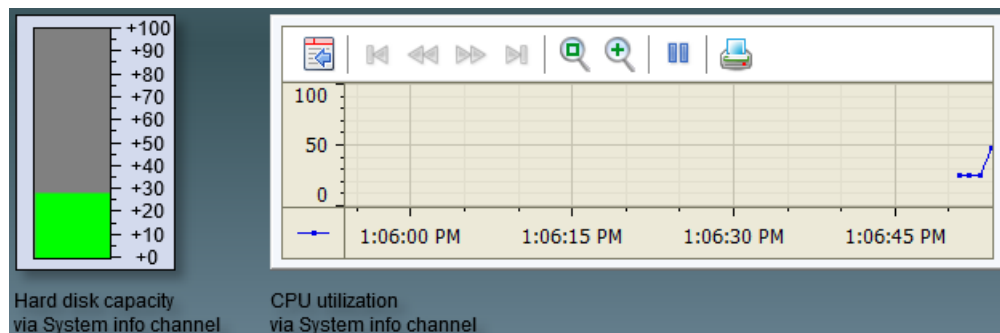
- WinCC Information System > Communication > Communication - Diagnostics > Diagnostics channel "SIMATIC S7-1200/S7-1500"

6.7.4 System information channel

The system information channel is used to evaluate system information such as hard disk 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 diagnostic picture along with the ActiveX control *Channel Diagnostics*.



Hardware diagnostics information for SIMATIC IPCs

SIMATIC industry PCs are equipped with the *SIMATIC IPC DiagBase* software. This software provides more information on the hardware than the system information channel, e.g.

- Display of status of a RAID hard drive system
- Display of temperatures of CPU or main board
- Display of the operating states or error states for fans / UPS / the SPS WinAC RTX if the corresponding hardware is used.

The *PCDiagBridge* (also known as *PCDiag*) software is an ActiveX application and offers a VBS-based programming interface. The information of the *SIMATIC IPC DiagBase* software can be displayed in SIMATIC WinCC either in process pictures or be processed in WinCC TagLogging or Alarm Logging.

See also

- WinCC Information System > Communication > System Info
- Diagnostics of SIMATIC IPCs, Online Support under entry ID 109478242 (<https://support.industry.siemens.com/cs/ww/en/view/109478242>)
- Diagnostic options for WinCC and PCS 7 OS, Online Support under entry ID 48698507 (<https://support.industry.siemens.com/cs/ww/en/view/48698507>)

6.7.5 Lifebeat Monitoring

The Lifebeat Monitor monitors all WinCC servers, WinCC 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 control level

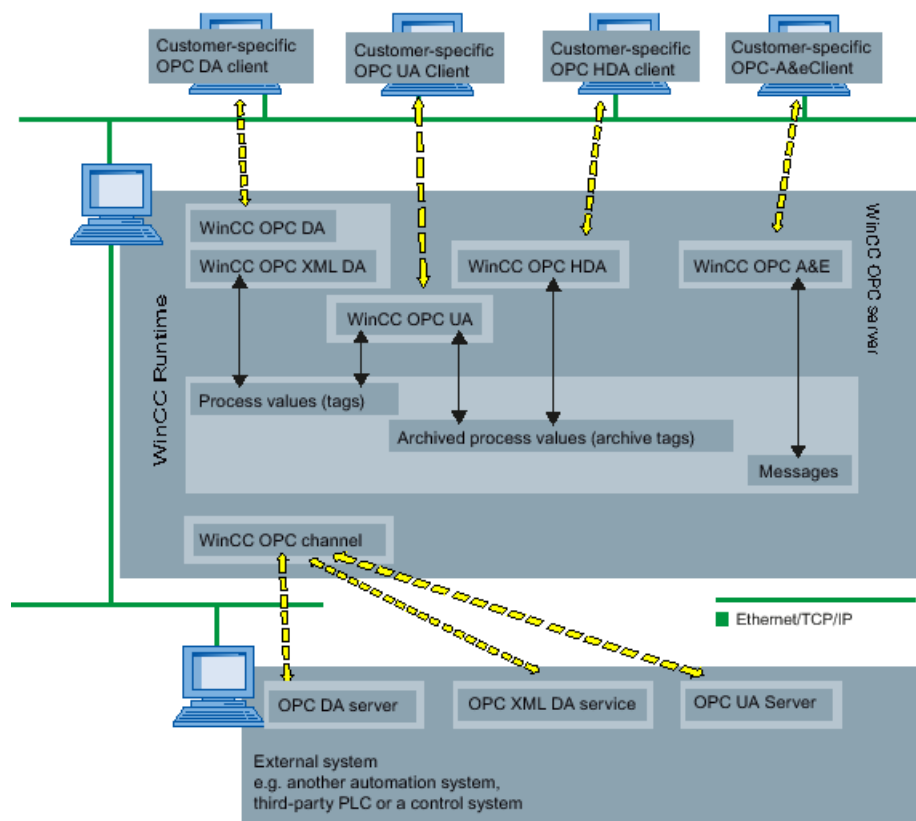
Data exchange with the plant control level or other systems can be covered by various system functionalities.

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): Access to the WinCC archive system (process values)
- OPC Alarms and Events (A&E): Access to the WinCC message system
- WinCC OPC UA Server: Access to the data management and archive system
- WinCC OPC DA / OPC XML DA Server: Access to the data management (license is already included in the WinCC RT license)
- WinCC OLE DB



See also:

- WinCC Information System > Options > Interfaces > OPC - Open Connectivity > Using OPC in WinCC

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 via web

With regard to web access by a computer in the network to a WinCC project, several WinCC options offer different possibilities.

Note

When using web access via a browser, ensure that the browser does not store passwords. This can be set in the respective browser.

WebNavigator / DataMonitor

While both read-only and read/write access can be set up with the WinCC/WebNavigator, the WinCC/DataMonitor option is also available as an alternative for read-only access.

See also

- WinCC Information System > Options > WinCC/WebNavigator
- WinCC Information System > Options > WinCC/DataMonitor
- Defense in depth, see section "Data and information security (Page 57)"

Note

The corresponding client has to be installed and licensed on the computer for remote access in order to view the process pictures in the Web client that are included in the ActiveX controls of the WinCC Premium Add-ons PM-CONTROL and PM-QUALITY.

WebUX

The WinCC option WebUX offers device- and browser-independent monitoring and control of WinCC Runtime for mobile devices.

Note

If operator input messages are to be created as audit trail entries via Web client or WebUX, the standard functions can be used (see chapter "Creating operator input messages (Page 80)").

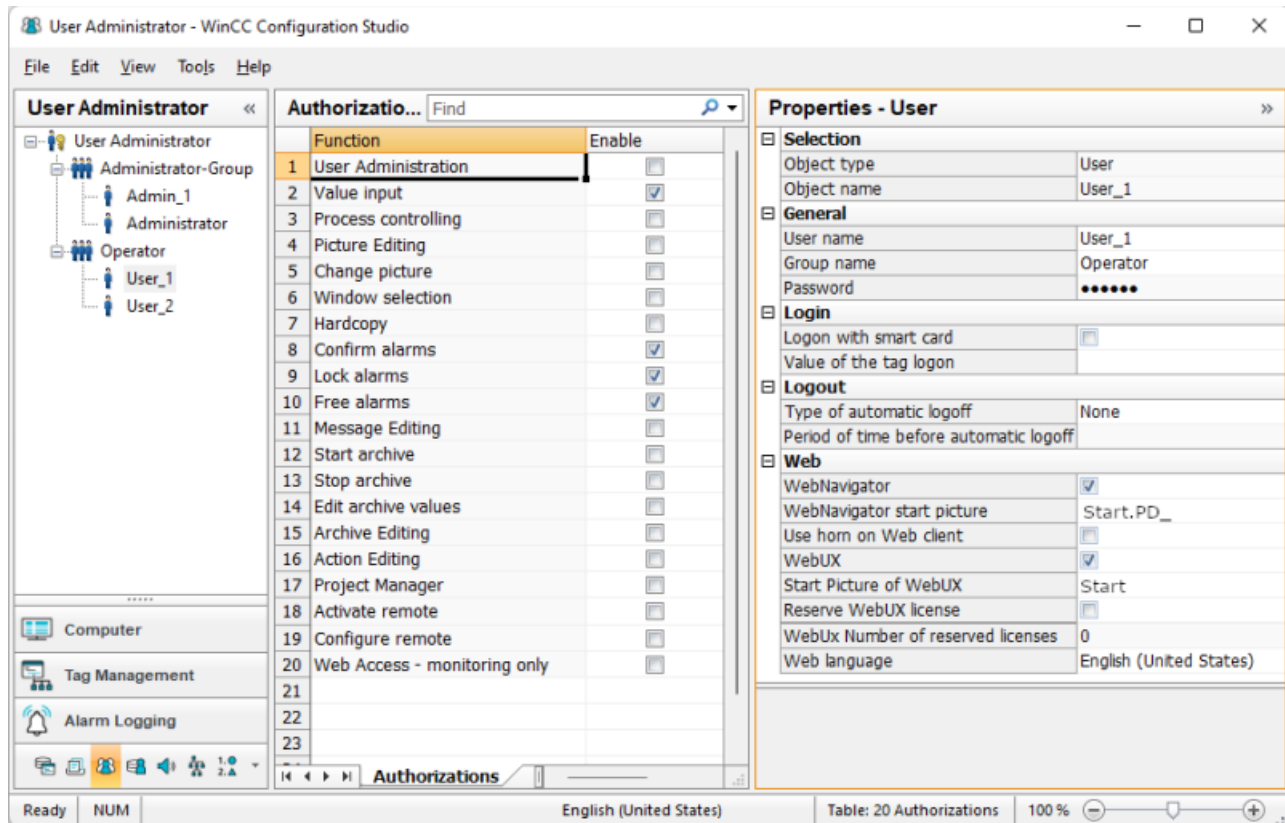
Supported functions and restrictions on web access with WebUX are shown by the WinCC Information System under

- Options > WinCC/WebUX - Supported functions in WebUX

6.9.1 Setting up user authorizations on the WinCC server

The operator authorizations in the Web client and via WebUX are set up in the WinCC User Administrator. When logging on to the web client and via WebUX, both SIMATIC Logon (user authentication) and the User Administrator in WinCC (operator authorization) check the authorization for the operation.

The "User Administrator" editor is opened in Configuration Studio.



In the properties of the user group, web access is enabled via the WebNavigator and/or via a WebUX connection. A start picture is configured for each option, which is displayed when web access is opened. The configured Web language applies to both options.

The "Web Access – monitoring only" function governs the user rights between WebNavigator and DataMonitor. If this function is not selected and the WebNavigator license is detected, the process pictures can be operated. 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 authorizations may differ for each user group.

Authentication of the user logged on via SIMATIC Logon is generally activated in the User Administrator and is also effective for logon via the Web client and the WebUX connection.

See also

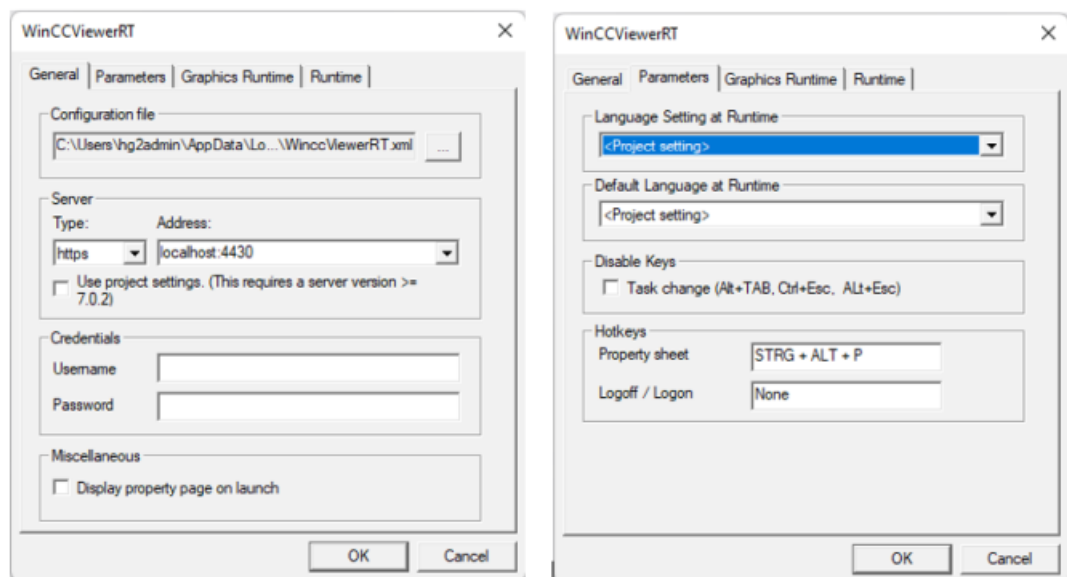
- Chapter "Configuration of SIMATIC Logon (Page 47)"

6.9.2 Remote access via the network with the WebNavigator

Remote access with the WebNavigator option requires the installation of the web client on the computer.

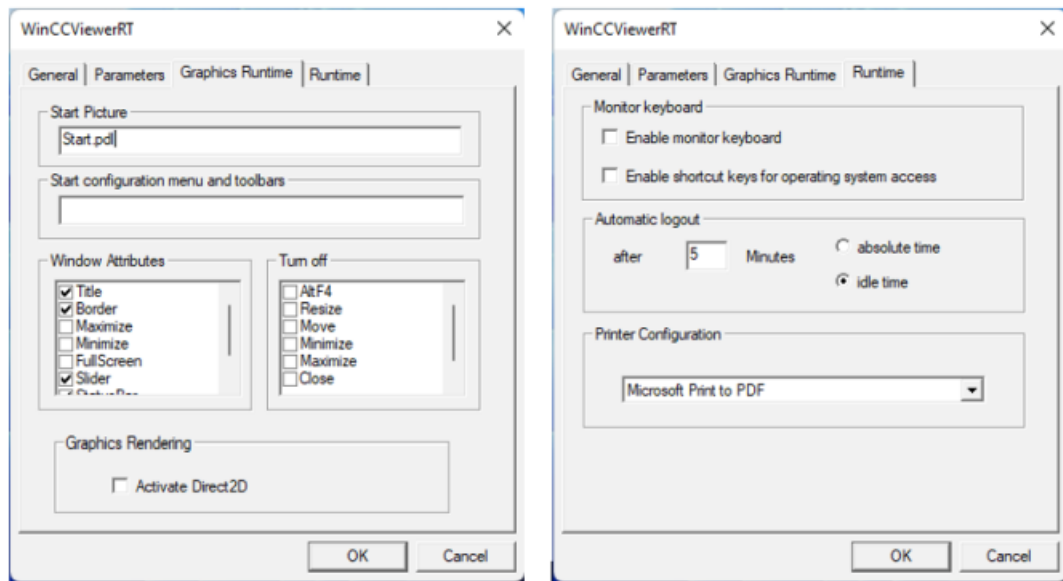
When the Web client is installed, a separate web view is automatically installed with the WinCCViewer RT application. As this can be customized, for remote access it is advisable to use the WinCCViewer RT application in preference to the Internet Explorer.

The WinCCViewer RT is started in the category "*Siemens Automation > WinCCViewerRT*" (dependent on the operating system). The first time this is called, parameters are assigned to the application via a configuration dialog:



If the same user always needs to be logged in when opening WinCCViewer RT, the user data can be specified in the "General" tab.

These fields are, however, not filled in for the logon/logoff of different users. A shortcut for logon/logoff can be defined in the "Parameters" tab. This shortcut key ends the current web session and opens the logon dialog for entering user data again. When the logon is successfully completed the WinCCViewer RT is opened for the newly logged-on user.



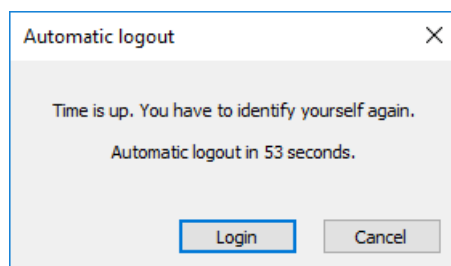
The contents of the WinCC controls can be output to a printer using the "Print" button. The printer is specified in the "Runtime" tab and must be available on the Web client computer.

The settings in the configuration dialog 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 or the logon dialog is opened. The configured parameter settings are set for future sessions. On the next start of WinCCViewer RT, the logon dialog is opened directly instead of the configuration dialog. If parameter settings need to be modified later, the configuration dialog is displayed with the shortcut key Ctrl+Alt+P. Alternatively, the XML file can be deleted in order to display the configuration dialog again when the WinCCViewer RT is started.

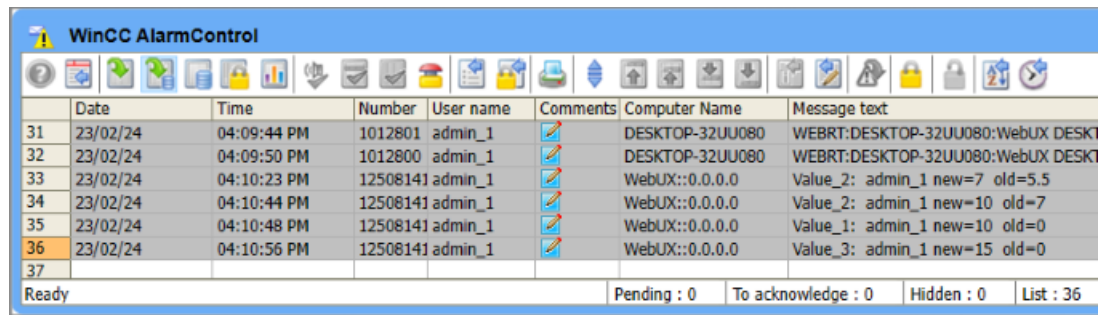
See also

- WinCC Information System > Options > "WinCC/WebNavigator > WinCC/WebNavigator Getting Started > Operating the WinCC project ...

The time configured for the automatic logout in the "Runtime" tab is relevant for the logout behavior of remote access via WinCCViewer RT. In the Web view, a message appears informing of the imminent automatic logout one minute before the configured time.



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



	Date	Time	Number	User name	Comments	Computer Name	Message text
31	23/02/24	04:09:44 PM	1012801	admin_1		DESKTOP-32UU080	WEBRT:DESKTOP-32UU080:WebUX DESK
32	23/02/24	04:09:50 PM	1012800	admin_1		DESKTOP-32UU080	WEBRT:DESKTOP-32UU080:WebUX DESK
33	23/02/24	04:10:23 PM	12508141	admin_1		WebUX::0.0.0.0	Value_2: admin_1 new=7 old=5.5
34	23/02/24	04:10:44 PM	12508141	admin_1		WebUX::0.0.0.0	Value_2: admin_1 new=10 old=7
35	23/02/24	04:10:48 PM	12508141	admin_1		WebUX::0.0.0.0	Value_1: admin_1 new=10 old=0
36	23/02/24	04:10:56 PM	12508141	admin_1		WebUX::0.0.0.0	Value_3: admin_1 new=15 old=0
37							
Ready						Pending : 0	To acknowledge : 0
						Hidden : 0	List : 36

To record the processes for establishing and terminating a connection via the web client in WinCC Alarm Logging, the WinCC system messages are activated in the Web settings for the WebNavigator in runtime. The system messages with the message numbers 1012400 and 1012401 are output and archived.

See also

- Chapter "Audit trail for operator actions (Page 84)"

6.9.3 Web access for data display

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

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

The Archive Connector tool is used to connect/disconnect the archived database with/from the Microsoft SQL Server.

6.9.4 Web access for mobile devices

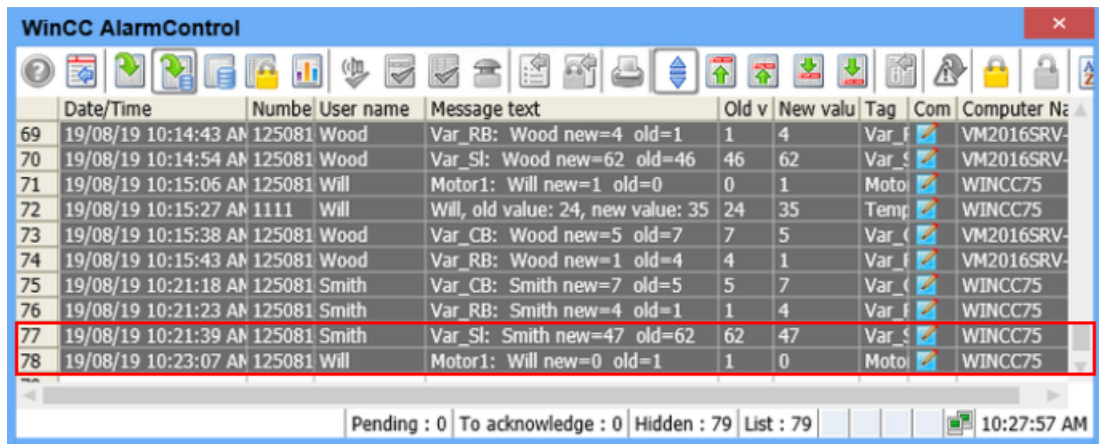
Web access via the WinCC/WebUX option does not require any software to be installed on the device, but is based on established web standards. Communication only takes place via a secure HTTPS connection with SSL certificates.

This access offers only limited functionality with regard to the display of graphic objects and controls in the process pictures and the editing of scripts.

See also

- WinCC Information System > Options > WinCC/WebUX - Documentation > Supported Functions

The user login is checked by SIMATIC Logon and the operator authorization by the WinCC User Administrator. Operator input controls on objects for which the standard operator input message and the Operator Activities Report have been activated, are recorded in WinCC alarm logging. The user who is logged on to WebUX is recorded in the operator input message. The Computer Name column shows the WinCC server and not the HMI device on which the operation was performed via WebUX.



	Date/Time	Numbe	User name	Message text	Old v	New valu	Tag	Com	Computer Na
69	19/08/19 10:14:43 AM	125081	Wood	Var_RB: Wood new=4 old=1	1	4	Var_f		VM2016SRV-
70	19/08/19 10:14:54 AM	125081	Wood	Var_SI: Wood new=62 old=46	46	62	Var_f		VM2016SRV-
71	19/08/19 10:15:06 AM	125081	Will	Motor1: Will new=1 old=0	0	1	Motol		WINCC75
72	19/08/19 10:15:27 AM	1111	Will	Will, old value: 24, new value: 35	24	35	Temp		WINCC75
73	19/08/19 10:15:38 AM	125081	Wood	Var_CB: Wood new=5 old=7	7	5	Var_f		VM2016SRV-
74	19/08/19 10:15:43 AM	125081	Wood	Var_RB: Wood new=1 old=4	4	1	Var_f		VM2016SRV-
75	19/08/19 10:21:18 AM	125081	Smith	Var_CB: Smith new=7 old=5	5	7	Var_f		WINCC75
76	19/08/19 10:21:23 AM	125081	Smith	Var_RB: Smith new=4 old=1	1	4	Var_f		WINCC75
77	19/08/19 10:21:39 AM	125081	Smith	Var_SI: Smith new=47 old=62	62	47	Var_f		WINCC75
78	19/08/19 10:23:07 AM	125081	Will	Motor1: Will new=0 old=1	1	0	Motol		WINCC75

Pending : 0 To acknowledge : 0 Hidden : 79 List : 79 10:27:57 AM

See also

- WinCC Information System > Options > WinCC/WebUX - Documentation

6.10 Interfaces to SIMATIC WinCC

6.10.1 Interfacing to SIMATIC WinCC

SIMATIC WinCC can also be used as a SCADA (Supervisory Control and Data Acquisition) system on which one or more lower-level HMI devices are connected. Messages and process values are transferred as packages. Online tags can be exchanged via the OPC interface or the WinCC Unified channel.

Central audit trail

Existing plants upgraded from WinCC V7.5 to V8.0 can still be operated with PM-OPEN IMPORT. In the process, the audit trail archive from WinCC RT Advanced or WinCC Comfort is generated as a circular archive in CSV format and imported by means of the PM-OPEN IMPORT into the database of WinCC Alarm Logging. More information on this procedure is provided in the GMP Engineering Manual of WinCC V7.5.

New systems, especially in combination with WinCC Unified, can use the WinCC Premium Add-on PM-ANALYZE to collect the audit trail from various stations in a central database in chronological order. In the process, the audit trails are exported cyclically into a compatible format by scripts. This can be transferred to the PM-SERVER File Control. The files exported from this are then imported by a lower-level component of the PM-ANALYZE, the PM-SERVER, and transferred into an alarm log.

The audit trails included in the alarm log of the PM-SERVER are either displayed and analyzed directly with PM-ANALYZE or transferred via further functions within the PM-SERVER to the Alarm Logging of WinCC. This way, the audit trails are also available for archiving with Process Historian.

See also

- FAQ "Import of Audit Trail from WinCC Unified into the PM Add-ons", Online Support under entry ID 109825543 (<https://support.industry.siemens.com/cs/ww/en/view/109825543>)

Central process value archiving and central alarm management

Existing plants upgraded from WinCC V7.5 to V8.0 can still be operated with PM-OPEN IMPORT. Exactly as with audit trail archives, tag and message archives, which are created in the lower-level HMI devices as short-term archives in CSV format, can also be transferred to the databases of SIMATIC WinCC with the PM-OPEN IMPORT add-on. Data from the data logs is entered in the WinCC Tag Logging accordingly and messages from the alarm logs are imported to WinCC Alarm Logging. Archive variables and messages must be created beforehand in WinCC. More information on this procedure is provided in the GMP Engineering Manual of WinCC V7.5.

PM-ANALYZE can be used for new systems to collect messages or process values from different operating devices in a central alarm or process value archive. The mechanism to import this data into the PM-SERVER is identical to the previously described procedure for audit trail. For archiving using Process Historian, the message data can be handed over to the WinCC Alarm Logging by means of function blocks of the PM-SERVER.

As part of Unified Collaboration, the tag communication between WinCC and WinCC Unified can also be enabled via the WinCC Unified Channel. Tags imported to WinCC can also be archived via the WinCC Tag Logging.

See also

- WinCC Information System > Communication > WinCC Unified Channel

6.10.2 Connection to 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.

In tag management, a connection is created for each automation system in the selected channel unit. The required tags can be imported directly for a connection to the SIMATIC S7-1200, S7-1500 channel unit. An online connection to the automation system is required. The PLC tags and contents of the data blocks are offered for selection via the shortcut menu *AS Symbols > Read from AS*. The selected tags are added as external tags in the WinCC tag management. PLC data types are transferred as structure tags.

If an online connection cannot be established, the data of the automation system can be exported to a file in the TIA Portal via the shortcut menu *Export to SIMATIC SCADA*, which is imported into WinCC tag management for the established connection. The contents of the file are once again offered for selection.

If the SIMATIC WinCC system is integrated in the SIMATIC Manager, all the tags relevant for WinCC are imported to WinCC.

Both in the case of integration in the SIMATIC Manager and a connection to a S7-1200/1500, the HMI tags are only maintained in the automation system.

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.

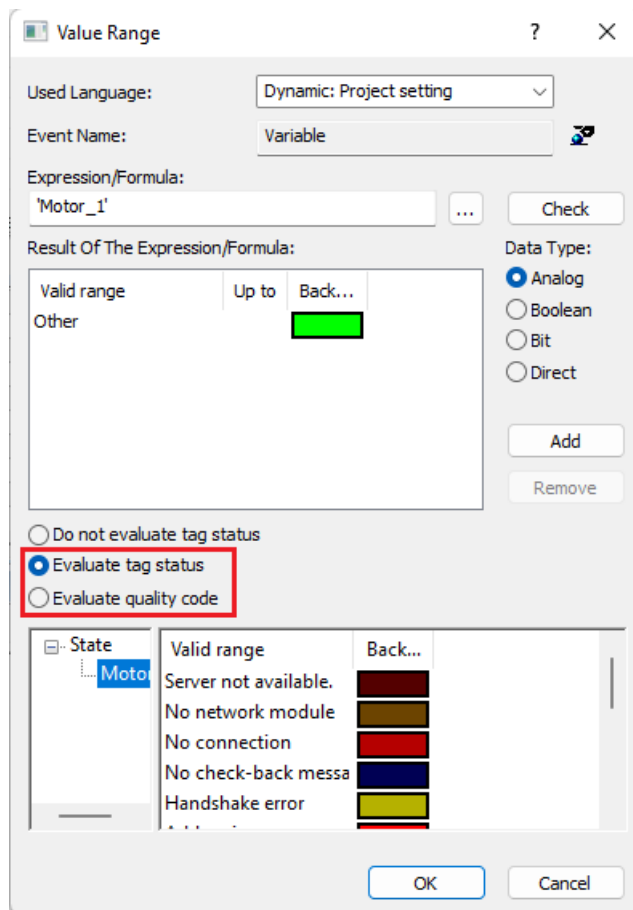
See also

- Manual "WinCC Configurations and Communication", Online Support under entry ID 109824642 (<https://support.industry.siemens.com/cs/de/en/view/109818894>)
- Chapter "Software components for engineering (Page 27)"

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.

Tag status or quality code for a tag can be monitored with the Dynamic Dialog. This is linked to an object property and configured accordingly. The following figure shows, for an I/O field, the Dynamic Dialog for the object property "Background color", which changes depending on the tag status.



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

- WinCC Information System > Working with WinCC > Dynamize Process Pictures > Dynamizing Using Dynamic Dialog > Monitoring Tag Status (or Monitoring Quality Code)

6.10.3 WinCC Cloud Connector

The WinCC Cloud Connector provides a connection to different clouds. This allows tag contents to be transferred cyclically and unidirectionally for display and analysis in a cloud. The enable for transmission and the cycle time are configured for each individual tag.

See also

- WinCC Information System > Interfaces > WinCC/Cloud Connector
- WinCC data connection to the cloud, Online Support under entry ID 109760955 (<https://support.industry.siemens.com/cs/ww/en/view/109760955>)

6.10.4 Interfacing third-party components

Connection via defined channels

OPC UA or OPC DA is recommended as the communication connection between WinCC and PLCs of other manufacturers. The corresponding communication drivers for OPC (OLE for Process Control) are certified by the OPC Foundation. The drivers for WinCC OPC DA clients and a WinCC OPC DA server are included in the scope of delivery of the WinCC system software.

The WinCC OPC client offers a connection to the OPC server, for example, to control systems of third-party manufacturers.

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

A connection via OPC UA (Unified Architecture) offers increased security in data communications compared with the OPC DA connection. OPC UA Server and OPC UA Client each provide a certificate. These certificates must be exchanged and accepted by the connection partners. Only then can successful data communication take place.

With the help of the WinCC/Connectivity Pack option, SIMATIC WinCC operates as an OPC DA/UA server and transfers process values to other OPC clients.

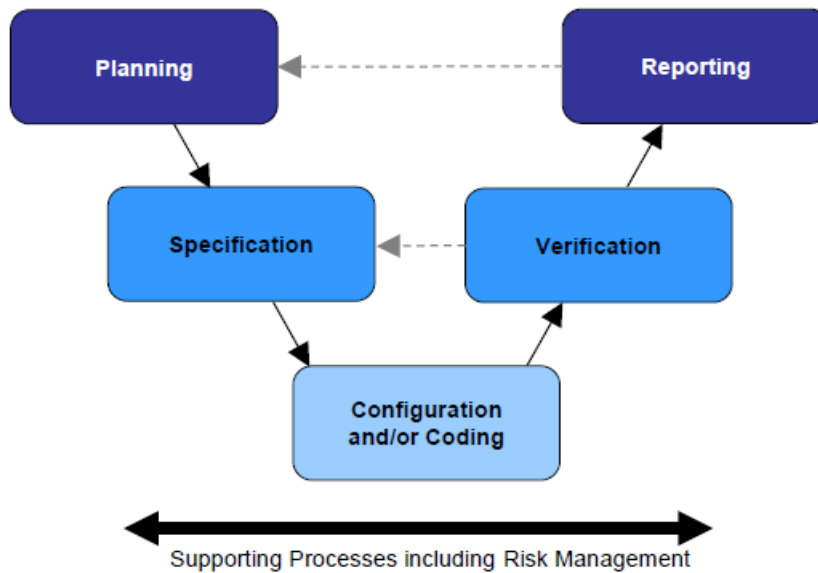
In WinCC tag management, each tag has the OPC write protection and OPC read protection properties. When activating the OPC read protection property, the tag is not visible for the OPC client. The activated OPC write protection property prevents the writing of tags from the OPC client.

See also

- WinCC Information System > Interfaces > OPC - Open Connectivity
- Chapter "Interfaces to process data (Page 33)"

Support for Verification

The following graphic shows an example of a general lifecycle approach. After specification and system setup, the system must be tested. GAMP 5 calls this phase the "Verification". The aim of verification is documented proof from testing (e.g. FAT, SAT) to ensure that the system meets specified requirements (URS, FS). 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.



Source: Figure 3.3, GAMP 5 – A risk-based approach to compliant GxP computerized systems

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

7.1 Test planning

In defining a project lifecycle, various test phases are specified. Therefore, basic activities (verification) 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 design, simulation)

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 no or only very few tests need to be repeated during subsequent test phases.

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 Verification of the hardware

Tests are performed to verify whether the installed components and the overall system design meet the requirements of the Design Specification. This covers such aspects as component designations, firmware/product version, location, server and clients used, interfaces, etc.

Verification of the employed PC hardware

The information below is an example of the data which should be specified and tested for verification of the PC hardware:

- Manufacturer/type designation/essential components
- Additionally installed hardware components (additional network adapter, printer, etc.)
- Verification of the configured network addresses, screen resolution, etc.

Verification of the network structure

The information below is an example of the data which should be specified and tested for verification of the network structure:

- Names of PC, clients, AS, etc.
- Type of connection and communication partner (Ethernet, OPC, etc.)
- TCP/IP address and subnet mask (when using clients)
- PROFINET device names

Supporting tools in the verification of the system hardware

- Printouts and screenshots as proof in the verification
- Additional visual checks of the hardware when necessary
- Printout of the SIMATIC NetPro configuration if WinCC is integrated in the SIMATIC Manager

- Overview of the configured interfaces with the application Siemens communication settings in the Siemens Automation category
- PC pass with information on all installed hardware and software components. This can be created manually or using commercially available tools.

7.3 Verification of the software

Supporting tools in the verification of the system software

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

- Installed software, see chapter "Verification of standard software (Page 116)"
- Report Designer, see chapter "Reporting with the WinCC Report Designer (Page 95)"
- SIMATIC Security Controller, see chapter "SIMATIC Security Controller (Page 41)"
- Diagnostics of communication connections, see chapter "Diagnostics of communication connections (Page 99)"
- System information channel, see chapter "System information channel (Page 100)"

7.3.1 Software categorization according to GAMP Guide

According to the GAMP 5 Guide, the software components of a system are assigned to one of four software categories for the purpose of validating automated systems.

See also

- GAMP 5 Guide, Appendix M4 "Categories of Software and Hardware"

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 be assigned to category 4 or sometimes even 5, the individual standard components to be installed (without configuration) can be handled similar to category 3 or 1.

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

If "free code" (VB/C script) is programmed as well, this corresponds to category 5 and involves significantly more effort for specification and testing.

Procedure for functions of category 5

Provision must be made to expend more effort for specification and testing:

- Creating a function description
- Execution according to the rules for script creation

- Comprehensive documentation of the program code
- Structural testing for compliance with rules
- Functional testing for compliance with the functional description

See also

- WinCC Information System > Working with WinCC > Dynamize Process Pictures > Configuration Recommendations
- WinCC Information System > Working with WinCC > ANSI-C for Creating Functions and Actions > Creating and Editing Actions > WinCC Coding Rule

7.3.2 Verification of standard software

During verification of the standard software in use, checks are made to verify whether or not the installed software meets the requirements of the specifications. These are usually products that are not specifically designed for a customer and which are freely available on the market:

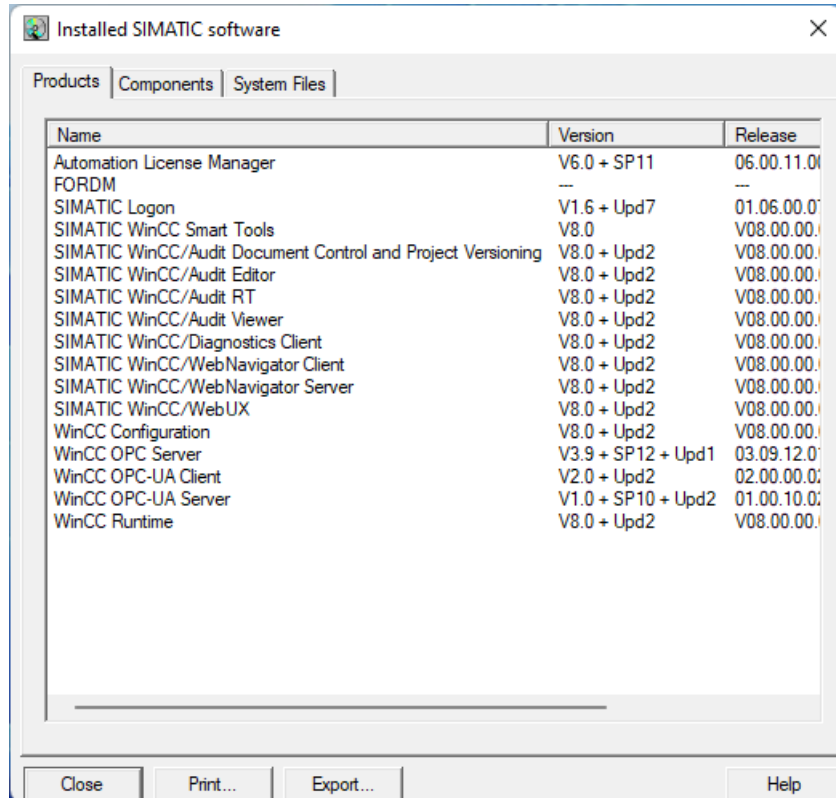
- Operating system and other software packages
- SIMATIC WinCC system software
- SIMATIC standard options (WebNavigator, WebUX, User Archives, etc.)
- SIMATIC WinCC Premium Add-ons (PM-CONTROL, PM-QUALITY, etc.)
- Standard libraries
- Third-party software such as Acrobat Reader, Microsoft Office (Word, Excel), etc.

Operating system and other software packages

The installed software can be verified by means of operating system functions. All installed software components are listed under Control Panel > Programs and Functions.

Installed SIMATIC software

Detailed documentation of the installed SIMATIC software can be found in the category Siemens Automation > Installed Software. The listing can be printed or exported.

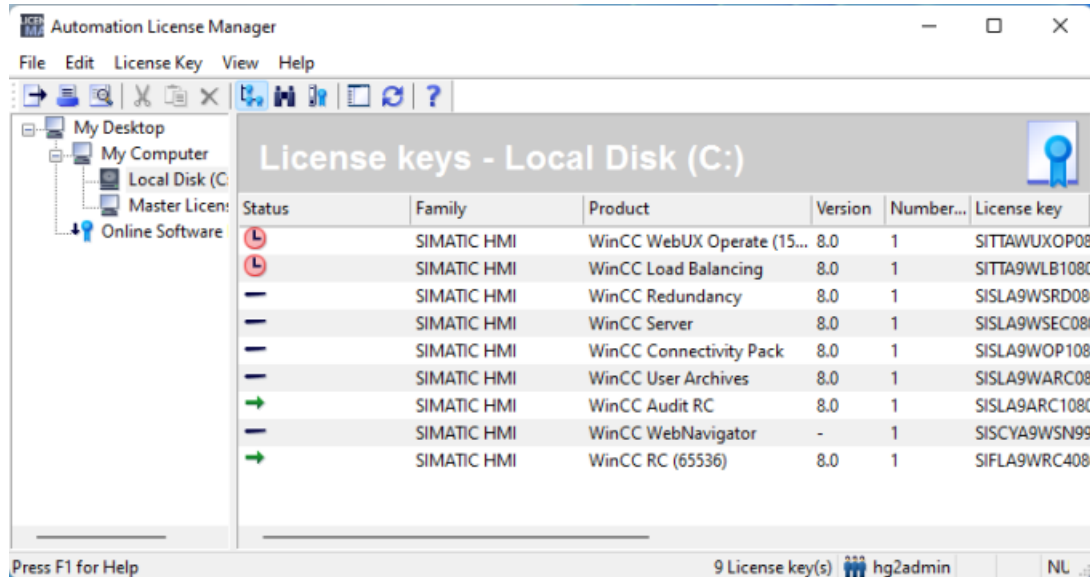


Name	Version	Release
Automation License Manager	V6.0 + SP11	06.00.11.00
FORDM	---	---
SIMATIC Logon	V1.6 + Upd7	01.06.00.00
SIMATIC WinCC Smart Tools	V8.0	V08.00.00.00
SIMATIC WinCC/Audit Document Control and Project Versioning	V8.0 + Upd2	V08.00.00.00
SIMATIC WinCC/Audit Editor	V8.0 + Upd2	V08.00.00.00
SIMATIC WinCC/Audit RT	V8.0 + Upd2	V08.00.00.00
SIMATIC WinCC/Audit Viewer	V8.0 + Upd2	V08.00.00.00
SIMATIC WinCC/Diagnostics Client	V8.0 + Upd2	V08.00.00.00
SIMATIC WinCC/WebNavigator Client	V8.0 + Upd2	V08.00.00.00
SIMATIC WinCC/WebNavigator Server	V8.0 + Upd2	V08.00.00.00
SIMATIC WinCC/WebUX	V8.0 + Upd2	V08.00.00.00
WinCC Configuration	V8.0 + Upd2	V08.00.00.00
WinCC OPC Server	V3.9 + SP12 + Upd1	03.09.12.00
WinCC OPC-UA Client	V2.0 + Upd2	02.00.00.00
WinCC OPC-UA Server	V1.0 + SP10 + Upd2	01.00.10.00
WinCC Runtime	V8.0 + Upd2	V08.00.00.00

The settings required in the Windows operating system for the WinCC system software can be queried in the SIMATIC Security Controller application: Category Siemens Automation > Security Controller (see also chapter "SIMATIC Security Controller (Page 41)")

SIMATIC software licenses

The SIMATIC tool **Automation License Manager** provides information on the installed licenses on the WinCC computer.



7.3.3 Verification of application software

For the verification of the application software, test descriptions are generated according to the stipulations of the software specification and the application software is tested based on these.

The following checks are typical when testing a computer system:

- Name of the application software
- Technological hierarchy (plant, unit, 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)
- Relationships between modes (MANUAL/AUTOMATIC switchovers, interlocks, start, running, stopped, aborting, completed etc.)
- Process tag names
- Visualization structure (P&ID representation)
- Operating philosophy (access control, group rights, user rights)
- Archiving concepts (short-term archives, long-term archives)
- Message concept

- Trends
- Time synchronization
- ActiveX controls from the PM products used

Project data such as the tags, functions or graphics used can be output based on reports. There are pre-configured standard layouts and print jobs for this that can be edited with the aid of the Report Designer. (see chapter "Reporting with the WinCC Report Designer (Page 95)")

7.4 Configuration control

7.4.1 Versioning

The type of versioning depends on the one hand on the system constellation and the tools used, on the other hand, the concept of data backup and versioning is usually also defined in the form of a work instruction or similar.

Manual project versioning

During data backup with the WinCC tool *Project Duplicator*, a version identifier can, for example, be integrated in the folder name into which the WinCC project is copied. When the WinCC project is duplicated, it has to be ensured that the WinCC project is closed.

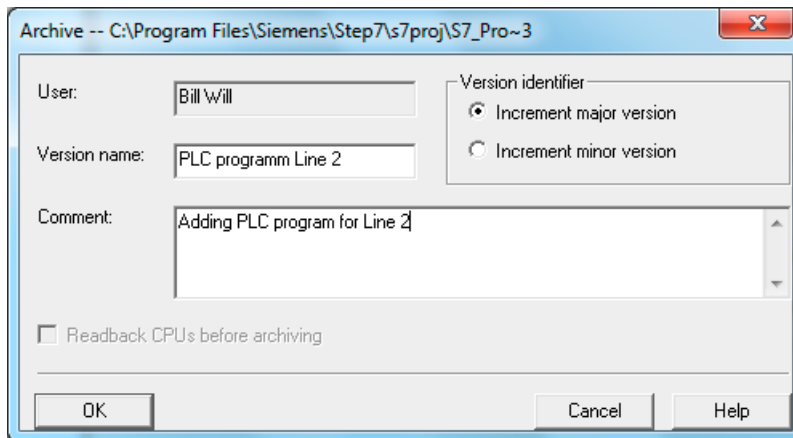
Versioning with "SIMATIC Version Trail"

A SCADA system SIMATIC WinCC, which is integrated in the SIMATIC Manager, is completely integrated in the STEP 7 project.

See also

- Chapter "Installation of SIMATIC components (Page 39)"

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.

	Action \	Name	Date	User	Readback	Status	Comment
1	New versioned ...	S7-Pro_Pharma	20.05.2015 13:11:38	CoCUser			C:\Program Files\Siemens\Step7\s7vtcom\S7-Pro_Pharma
2	New archive	\S7_Pro_Pharma	20.05.2015 13:15:29	CoCUser		New	Project '\S7_Pro_Pharma' pasted.
3	Archive version	\S7_Pro_Pharma	20.05.2015 13:35:58	Bill Will	not executed	OK	\S7_Pro_Pharma 1.0 C:\Program Files\Siemens\Step7\s7proj\S7_Pro~3
4	Archive version	\S7_Pro_Pharma	20.05.2015 14:15:02	Hans Meier	not executed	OK	\S7_Pro_Pharma 1.1 C:\Program Files\Siemens\Step7\s7proj\S7_Pro~3
5	Archive version	\S7_Pro_Pharma	20.05.2015 14:23:35	Hans Meier	not executed	OK	\S7_Pro_Pharma 1.2 C:\Program Files\Siemens\Step7\s7proj\S7_Pro~3
6	Archive version	\S7_Pro_Pharma	05/20/2015 02:32:11...	Bill Will	not executed	OK	\S7_Pro_Pharma 2.0 C:\Program Files\Siemens\Step7\s7proj\S7_Pro~3

When using SIMATIC Version Trail for continuous archiving, the version history provides a good way of documenting various software states 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 PCS 7, Online Support under entry ID 109811153 (<https://support.industry.siemens.com/cs/ww/en/view/109811153>)

Versioning of data in WinCC options / Add-ons

The project data for Premium Add-ons (PM-QUALITY, etc.) that are integrated directly in the WinCC project are also backed up and versioned during the manual data backup with the Project Duplicator or in a compressed file. The requirement here is also that all participating applications are closed and the databases are disconnected from the Microsoft SQL Server. If the project of the PM product is maintained in a separate project path, away from WinCC, this project path must be saved manually (Zip file) and versioned in the storage path name.

See also

- Chapter "Data backup of the application software (Page 124)"

Versioning of configuration elements

Configuration can be checked with the help of versioning of the individual configuration elements and the associated change documentation, for information see chapter "Versioning application software (Page 71)".

7.4.2 Change control

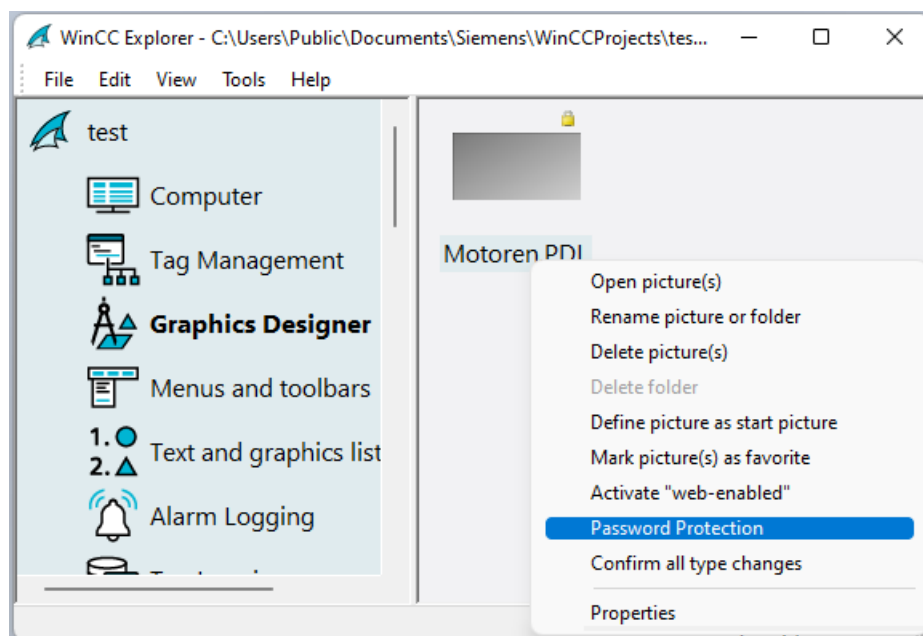
Some third-party software from third-party providers on the market provide good and useful supplements to the functionality of SIMATIC WinCC. The functional scope ranges from individual special supplements to comprehensive tools for data backup, change control and software versioning of different systems. In this way, you can compare two different versions of a project with each other and show their differences.

7.4.3 Write protection

You can assign a password to one or more pictures and faceplate types from the shortcut menu of the "Graphics Designer" entry in the data window of the WinCC Explorer.

See also

- System manual "Working with WinCC", chapter 4.5.12, Online Support under entry ID 109824649 (<https://support.industry.siemens.com/cs/ww/en/view/109818253>)



Data Backup

Periodic data backups are not only necessary to avoid data loss during the configuring phase. They are also necessary during the operation phase to ensure a smooth system restoration in the event of data loss or system failure. An emergency plan is also required for this case.

In addition to backing up the system installation, the configuration should also be backed up regularly, for example, to be able to access the last current system configuration after a hardware defect or data loss.

The following data backups should be considered:

- Backups of the system installation, see chapter "Backup of the system installation (Page 123)"
- Backup of the installation, including all project files (image)
 - following system updates and major project changes
 - as well as periodically, e.g. every 12 months
- Change-driven backup of project data before/after every change
- Periodic backup or "recopying" of all archived data every 3 to 5 years, for example, to ensure the readability of the data.

Note

The backup of the user software and the backup of the system partition with and without SIMATIC installation should be stored on external media (for example, CD, DVD, network backup).

See also

- Chapter "System restoration (Page 128)"

8.1 Backup of the system installation

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.

Which images are advisable?

- Creation of an image of the operating system installation with all drivers and all settings for the network, user administration, etc., without SIMATIC installation
- Creation of an image of the PCs with SIMATIC installation
- Creation of an image of the PCs with SIMATIC installation including all projects

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.

8.2 Data backup of the application software

It is advisable to generate regular data backups of the project data. In this storage concept, it might be specified, for example, that the project is backed up following a change. This project backup can be performed in several different ways.

Manual project backup

If the project is backed up with the WinCC tool "**Project Duplicator**", a direct copy of the WinCC project is created in the specified path. The WinCC project must be closed before it is copied. The project backup also includes the project library and global VB / C scripts. The global library is maintained outside the WinCC project in the WinCC installation path in the aplib folder and therefore has to be backed up separately.

By using the "**Copy Project**" application, it is, however, possible to back up the entire WinCC project including all databases during runtime operation. The backup is triggered either manually or automatically by call in a WinCC action and is made in a directory specified by the user, which is supplemented by the current date time stamp.

See also

- FAQ "Backup WinCC project during operation", Online Support under entry ID 38493803 (<https://support.industry.siemens.com/cs/ww/en/view/38493803>)

As an alternative, the folder containing the WinCC project can be compressed in a file in Windows Explorer either with Windows methods or a suitable tool to back up a project.

See also

- FAQ "Data backup of the WinCC project on the OS", Online Support under entry ID 109766573 (<https://support.industry.siemens.com/cs/ww/en/view/109766573>)

Data backup with SIMATIC Version Trail

The SIMATIC Version Trail option can be used to perform a manual or scheduled back up of the project. An older version can also be restored via the interface. Version Trail is a software option for the SIMATIC Manager.

See also

- Chapter "Versioning (Page 119)"

Data backup in WinCC options / Add-ons

If options or Premium Add-ons such as PM-CONTROL, PM-QUALITY or PM-ANALYZE are used in the WinCC project, the corresponding databases must also be backed up. To do so, the project must be closed in PM-SERVER, the utility application to the PM Add-ons, before the data backup, in order to disconnect the databases from the Microsoft SQL Server.

The directory that contains the project data of the Add-ons (by default: C:\Users\Public\Documents\Siemens\ProcessManagement\...), is copied or compressed. If file names have been changed during this, the original names of the directories must be reset before the data can be restored.

If the Premium Add-on PM-OPEN IMPORT is used, the configuration file (by default this file is called *Project.csv*) is saved to the configured storage location.

The "Copy Project" application can also be used to back up the databases of the WinCC Premium Add-ons in online operation. If the Premium Add-ons PM-QUALITY, PM-CONTROL and PM-ANALYZE are integrated directly in the WinCC project, the databases of the Premium Add-ons are included automatically when backing up the WinCC project with WinCC Copy Project.

Handling of the database in the WinCC/Audit option is described in the respective system manual, including backup and restoring.

Operation, Maintenance and Servicing

9.1 Operation and monitoring

9.1.1 Process visualization

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

Production can be monitored, controlled and optimized with versatile interfaces. The central components in monitoring during operation are screen signals in graphics and faceplates along with trends, messages, acoustic signals etc. With the ActiveX Assigned Control *PLCCodeViewerControl* SIMATIC WinCC offers the mapping of a network from a SIMATIC PLC in an operator control picture without STEP 7 installation.

Runtime data can be output by the system based on reports. There are pre-configured standard layouts and print jobs for this that can be edited with the aid of the Report Designer. (see chapter "Reporting with the WinCC Report Designer (Page 95)")

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.

9.1.2 Audit trail review

In a regulated environment, it is necessary not only for an audit trail for changes to GMP-critical data to be kept, but also for this audit trail to be checked regularly. On the one hand, this can take place through regular review of the functionality with simultaneous incorporation of the relevant audit trails into relevant production reports. On the other hand, evaluations of critical alarms, operator inputs and frequency analyses of messages can also serve to improve the process.

The audit trail review can be aided by:

- Possible contents of an audit trail, see chapter "Audit trail and change control (Page 84)"
- System diagnostics, see chapter "Monitoring the system (Page 98)"
- Logging options, see chapter "Reporting (Page 94)"
- Comprehensive analysis of messages from a wide range of sources using the WinCC Add-on PM-ANALYZE (Page 37)

9.2 Operational change control

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

The procedure for changes comprises the following steps:

1. Initiation, description and approval of planned change by plant user
2. Check and backup of the current application software version (project data)
3. Adapting the system specifications
4. Executing the change, including documentation of the performed change
5. Testing the change, including test documentation in suitable form
6. Backup of the changed project with new version ID

The effects of the change to other parts of the application and the resulting tests must be specified based on risk and documented.

It is advisable to categorize various actions and measure the change effort for the risk. In the case of a 1:1 exchange of a hardware component, for example, the risk must be lower than with different components.

Moreover, in the case of software updates, it might be necessary to make a choice between system security and conformity with the regulations, see also chapter "Updating the system software (Page 132)".

9.3 System restoration

Data backups are used to restore the system after failure. The backup data (medium) and all the materials needed for the restoration (basic system, loading software, documentation) must be saved at the defined point.

System failure (also referred to as a disaster) can be caused by the following, for example:

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

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 image (see chapter "Backup of the system installation (Page 123)"). The instructions provided by the relevant software supplier for the data backup application should be followed.

If a PC with an identical hardware configuration is not available, the installation has to be run again from scratch. The documentation that contains descriptions of the installed software and the updates, upgrades and hot fixes also installed, can be used to qualify the software.

Restoring the application software

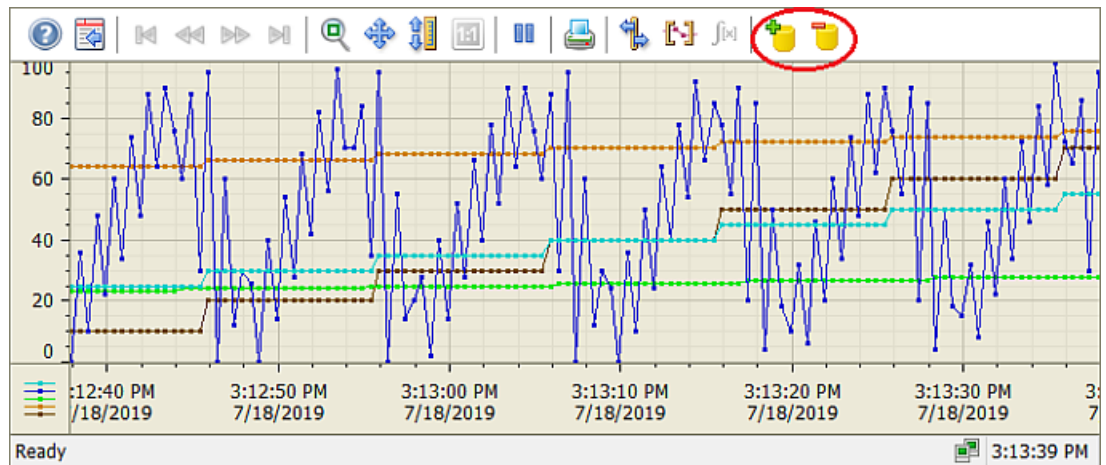
The process for restoring the application software depends on the kind of backup.

- Reading back data from a manually created backup state (Project Duplicator, Copy Project, compressed file)
- Reading back the data using the software Version Trail when SIMATIC WinCC is operated integrated in the SIMATIC Manager
- If required, 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 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 historical data in WinCC Runtime, corresponding backup states with the extension *mdf* and *ldf* are copied back to the local computer and linked to the Microsoft SQL Server using the *Connect archives* button in the controls.



When using a Process Historian, the data does not have to be copied back. The data is displayed directly in the ActiveX controls *WinCC Alarm Control* or *WinCC Trend Control / Table Control* by selecting the historical 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 Process Historian

The best way to avoid data loss due to hard disk defects is to use RAID systems. The Process Historian can also be operated as a redundant archiving system.

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

9.4 Uninterruptible power supply

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.

9.4 Uninterruptible power supply

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 recording in the battery backup. The reporting should also record 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

System Updates and Migration

10.1 General procedure

It is essential that system software updates for a validated plant are agreed with the user or are initiated by him. 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 "Operational change control (Page 128)", this roughly means the following steps:

- Describe the planned change
- Effect on functions / plant units / documentation, for example, including the system description of the new and modified functions in the readme file/release notes for system updates
- Effect on readability and availability of archived data
- Assessment of the risks for the overall process and the validated status
- 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)
- Updating of existing system description and preparation of the test documents
- Perform data backup before the update
- Make the change following plant release
- Accompanying documentation of the activities performed
- Perform and document the required tests (verification)
- Perform new data backup, possibly including system image

In considering possible influences on the application, the following may be relevant:

- Modules and libraries, classes and instances
- Process pictures, graphic settings, objects, script-based dynamization
- Alarm system and process value archiving in function and display
- Operator authorizations
- Interfaces
- Effects during download
- System performance
- Documentation (specifications)
- Verification tests to be repeated or performed for the first time

10.2 Updating the system software

Updates of the system software may be, for example:

- SIMATIC WinCC updates, service packs and new versions
- Updates of standard software such as Microsoft Office or virus scanners
- Operating system updates

In addition to improvement to security aspects and corrections of error, the scope of functions can be extended or improved.

When there is an update of the WinCC system software, it may be necessary to migrate or convert configuration data of the project of the older version, see chapter "Migration of the application software (Page 132)".

In the case of a larger version change, it is also possible that an upgrade must be made to an interim version and then to the target version afterwards.

See also

- WinCC Information System > Getting Started > Migration
- "Microsoft Patches (security updates)", Online Support under entry ID 18752994 (<https://support.industry.siemens.com/cs/ww/en/view/18752994>)
- GAMP 5 Guide, Appendix S4 "Patch and Update Management"

Note

The SIMATIC Industry Support (<https://sieportal.siemens.com/en-ww/home>) provides support for software updates and project migration.

10.3 Migration of the application software

In addition to the system software, the application software may also be affected by an update, as mentioned above. The scope can range from a mere migration of data, file formats or storage media, through the migration of databases and project data, all the way to complex system migrations including hardware and operating system changes. Migration is understood as the transition to a technical successor generation.

Migration of the WinCC project data

The *Project Migrator* application is available for the migration of a WinCC project from a previous version to the current SIMATIC WinCC version. 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.

See also

- Migration of WinCC Projects from V4 to V8, Online Support under entry ID 44029132 (<https://support.industry.siemens.com/cs/ww/en/view/44029132>)

Migration of the project data from Premium Add-ons

The conversion of the project data from the immediately preceding version to the current product version can be performed automatically in the new version. A direct migration from older product versions to the current version is not possible. In this case, the WinCC Competence Center (email to WinCCAddon.automation@siemens.com) offers migration subject to a fee.

10.4 Validation effort for migration

System updates and migrations must be planned, checked and documented. The validation effort must be decided in consultation with the plant operator. The technical expertise usually comes from the system supplier.

Depending on the scope of the update, the following documents are created:

- Change request of the user, see chapter "Operational change control (Page 128)"
- Migration plan or update plan
- Checklist for installation / migration
- Test specification to ensure functionality after update
- Test results together with attachments and deviations
- Final report

Test points in the verification

The following test points may be relevant in the test specification to verify the changes made:

- Proper installation of the required software components
- New or changed system functions of this version
- Basic functionality of the system, from a technical and user point of view
- GMP-critical functions and parameters, archiving and reports, also the readability of archived data
- Sample tests for automated migration
(The migration functionality provided by the system is a product feature that does not require testing in detail in the project application.)
- Manual adjustments made in addition to automatic migration must be described, documented and tested separately in accordance with change control procedure.

The steps in chapter "General procedure (Page 131)" must be taken into consideration.

Note

As a rule of thumb: The higher the manual engineering effort for a migration/update, the higher the associated validation work for the preparation, subsequent test and documentation.

Abbreviations

Abbreviation	Description
AS	Automation System
CFC	Continuous Function Chart
CFR	Code of Federal Regulations (USA)
CSV	A file format, but also used for Computerized System Validation
DS	Design Specification
EU	European Union
FAQ	Frequently Asked Question
FAT	Factory Acceptance Test
FDA	Food and Drug Administration (USA authority)
FS / FDS	Functional Specification / Functional and Design Specification
GAMP	Good Automated Manufacturing Practice
GMP	Good Manufacturing Practice
HDS	Hardware Design Specification
HMI	Human Machine Interface
MES	Manufacturing Execution System
OLE	Object Linking and Embedding
OPC	OLE for Process Control
OS	Operator Station
PLC	Programmable Logic Controller
P&ID	Piping and Instrumentation Diagram (plant overview)
RT	Runtime
SAT	Site Acceptance Test (part of acceptance test)
SDS	Software Design Specification
SFC	Sequential Function Chart
SOP	Standard Operating Procedure (working instructions)
SVG	Scalable Vector Graphics
URS	User Requirements Specification
UPS	Uninterruptible Power Supply
UTC	Universal Time Coordinated
VBA	Visual Basic for Applications

Index

A

- Access control, 17
- Access protection, 42
- Alarm Logging, 28, 69
- Antivirus, 61
- Application software, 77
- Archive
 - Audit trail, 108
 - Process values, 91, 109
 - Short-term archive, 92
- Archiving, 20, 90
 - Long-term archiving, 93
- Audit trail, 18, 19, 84
- Availability, 32

B

- Backup, 123
- Batch report, 19
- Batch-based control, 36

C

- Category
 - Hardware, 15
 - Software, 15
- Change control, 13, 128
- Channel Diagnostics, 99
- Configuration management, 16, 71
- Configuration Studio, 27
- Connectivity Station, 102

D

- Data backup, 20, 38, 124
- Data exchange, 101
- Defense in depth, 59
- Diagnostics, 99
- Disaster recovery, 128

E

- Electronic records, 18
- Electronic signature, 18, 88
- Engineering Software, 27

EU GMP Guide Annex 11, 11, 18

F

- Faceplate, 64
- FDA 21 CFR Part 11, 11, 18
- Firewall, 61

G

- GAMP 5, 12
- GMP requirements, 15
- Graphics Designer, 66, 72, 79
- Guidelines, 11

H

- Hardware, 24
- Hardware category, 15

I

- Image, 38, 123
- Industrial Security Services, 59
- IndustrialDataBridge, 102
- Information Server, 31
- Installation
 - Operating system, 39
 - SIMATIC Security Controller, 41
 - SIMATIC WinCC, 40
 - SIMATIC WinCC Add-ons, 42
 - SIMATIC WinCC options, 42
- Interface
 - Process data, 33
 - S7, 109
 - Third-party component, 111

L

- Library, 66
- Lifebeat Monitoring, 101
- Lifecycle model, 11
- Long-term archive server, 30
- Long-term archiving, 30, 37, 42, 93

M

Migration, 131, 132
Monitoring, 99

O

Object-oriented configuration, 64
Operator input message, 80
Overview pictures, 77

P

Page layout editor, 96
Partition, 38
Password, 17
Performance tags, 98
Picture window, 65
Print jobs, 96
Process Historian, 30, 94
Process pictures, 77
Project settings, 63

Q

Quality code, 110

R

Redundancy, 67
Regulations, 11
Report Designer, 31, 95
Reporting, 31, 36, 95, 96
Restoration, 128
Retrieving data, 21
Risk analysis, 13, 114

S

SCALANCE S, 58
Scripts, 66, 73
Security, 25
 Access control, 17
Security by default, 61
SICLOCK, 69
SIMATIC Logon, 27, 47
Software category, 15, 115
Specification, 23, 26

Structure tag, 65
Supplier audit, 21
System installation, 39
System updates, 131

T

Tag Logging, 29, 70
Test planning, 113
Third-party components, 21
Time stamp, 69
Time synchronization, 21, 68
Type/instance concept, 16

U

Uninterruptible power supply, 130
UPS, 130
User administration, 27, 42
 Security settings, 45, 50
User groups, 46
User ID, 17
User management, 17
User objects, 64
User rights, 50

V

Validation Manual, 12
Verification, 113
 Application software, 118
 Standard software, 116
Version Trail, 119, 124
Versioning, 119
 Application software, 71
 Configuration elements, 71
 Pictures, 72
 Reports, 75
 Scripts, 73

W

Web access
 Data display, 107
 Operator authorizations, 104
 Remote, 105
Web client, 103
Whitelisting, 61
WinCC Add-on
 Data Backup, 125

- PM-ANALYZE, 31, 37
- PM-CONTROL, 36
- PM-OPEN IMPORT, 37, 108
- PM-QUALITY, 36, 37, 68, 94, 96
- Versioning, 121
- WinCC Certificate Manager, 61
- WinCC option
 - Audit, 29, 87, 89
 - Connectivity Pack, 34, 101
 - DataMonitor, 30, 33, 103
 - Open Development Kit (ODK), 102
 - PerformanceMonitor, 33
 - Redundancy, 32
 - User archives, 29, 92
 - Versioning, 121
 - WebNavigator, 33, 103
 - WebUX, 107
- WinCCViewer, 105

Get more information

Siemens AG
Digital Industries
Pharmaceutical and Life Science Industry
Siemensallee 84
76187 Karlsruhe, Germany
PDF (A5E53427495-AA)
Produced in Germany

Subject to changes and errors. The information given in this catalog only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products.

The requested performance features are binding only when they are expressly agreed upon in the concluded contract. All product designations may be trademarks or product names of Siemens AG or other companies whose use by third parties for their own purposes could violate the rights of the owners.