SIEMENS

SIMATIC

SIMATIC WinCC (TIA Portal) V15

Guidelines for Implementing Automation Projects in a GMP Environment

GMP Engineering Manual

Edition 03/2019

Answers for industry.

SIEMENS

SIMATIC

WinCC (TIA Portal) V15 GMP Engineering Manual

Configuration Manual

Guidelines for Implementing Automation Projects in a GMP Environment

03/2019
A5E44854710-AA

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 AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

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

Siemens AG
Division Process Industries and Drives
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E44854710-AA
℗ 03/2019 Subject to change

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 and STEP 7 is required to understand this manual. Knowledge about GMP in the pharmaceutical industry is also beneficial.

Validity of the manual

The information described in this manual is evaluated exemplary for SIMATIC WinCC / STEP 7 (TIA Portal) V15 for the following components:

- Server/client system configured with the engineering software SIMATIC WinCC Professional
- Panel TP1200, configured with the engineering software SIMATIC WinCC Comfort
- SIMATIC S7-1500, configured with the engineering software SIMATIC STEP 7 Professional

with the options WinCC Recipes, WinCC WebNavigator and WinCC Audit as well as the WinCC Premium Add-ons PM-CONTROL, PM-QUALITY, PM-OPEN IMPORT, PM-ANALYZE and PM-LOGON.
Information regarding the exact compatibility between the various components is contained in the product catalog CA 01 (http://www.siemens.com/automation/ca01).

The TIA Selection Tool (https://w3.siemens.com/mcms/topics/en/simatic/tia-selection-tool) guides you through an error-free configuration using intelligent configurators and selection wizards.

A list of the compatibility of different product versions can be accessed under (http://www.siemens.com/kompatool).

Any requests about the compatibility of the Premium Add-ons for SIMATIC WinCC should be addressed directly to the suppliers or checked in the TIA Selection Tool, see here (http://w3.siemens.com/mcms/human-machine-interface/en/visualization-software/scada/wincc-addons/Pages/Default.aspx).

Position in the information landscape

The system documentation of the SIMATIC WinCC (TIA Portal) operator control and monitoring system is an integral part of the system software. The TIA Portal information system is available to the user as online help (HTML help) or as electronic documentation in PDF format.

This manual supplements the existing SIMATIC WinCC manuals. It serves not only as a guideline for configuring, but also provides an overview of the requirements for configuring 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

We offer various courses to help you get started with SIMATIC WinCC (TIA Portal). Please contact your regional training center, or the central training center in D 90327 Nuremberg.

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

Siemens on the Internet

The guide to the technical documentation of various SIMATIC products and systems can be found here (https://support.industry.siemens.com/cs/ww/en/view/65601780) or in the Online Support under entry ID 90939751 (https://support.industry.siemens.com/cs/ww/en/view/90939751).

You can find the online catalog and online ordering system at (http://mall.industry.siemens.com/) or in the TIA Selection Tool (https://w3.siemens.com/mcms/topics/en/simatic/tia-selection-tool).

For more information about Siemens products for the pharmaceutical industry, see here (http://www.siemens.com/pharma).

You can access the WinCC Center of Competence in Mannheim on the Internet under (www.siemens.com\Process-Management) or by e-mail at WinCCAddon.automation@siemens.com

Technical support on the Internet

You can find comprehensive information about our Service and Support at: (http://support.industry.siemens.com)

The product support offered there includes:

- Technical specifications and information on the product status
- FAQs and application examples

You can also find on this page:

- Application examples
- 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: (http://www.siemens.com/automation/partner)

If you have questions on the manual, please contact:

E-mail: pharma@siemens.com

Table of contents

Configuring in a GMP Environment 1

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:

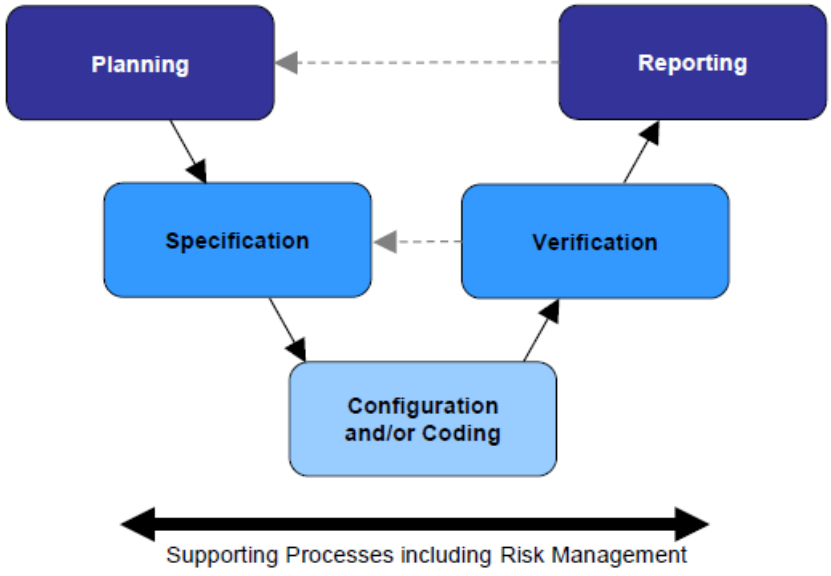
Title (Author)	Subtitle	Area of application
21 CFR Part 11 (US Food and Drug Administration, FDA)	Electronic Records, Electronic Signatures	Law/regulation for manufacturers and importers of pharmaceutical products for the U.S. market
Annex 11 of the EU GMP Guide (European Commission)	Computerised systems	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.

GAMP 5 approach

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.



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

The lifecycle approach illustrated here is known as a generic model in GAMP 5. With this as the basis, we will introduce several examples of lifecycle models for a variety of "critical" systems with different stages of specification and verification phases.

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

Siemens Validation Manual

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.

1.3 Responsibilities

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.

See also

- 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 the 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 25)“.

2.1 Categorization of hardware and software

Hardware categorization

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

Software categorization

According to the GAMP Guide, the software components of a system are divided into various software categories. These 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 Guide 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 19)
- RFID / smart cards together with a password
- Evaluation of biometrics, e.g. fingerprint scanners

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.

2.5.1 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
- Use of numerals (0-9)
- Use of special characters

See also

- Chapter "Setting up user administration (Page 48)"

2.5.2 Application of access control to an automation system

In addition to physical Access protection control, automation systems of the SIMATIC S7-1500 provide access protection through the display protection on the device and through assignment of software passwords in different protection levels for access to program data via the network.

See also

- Chapter "Protection functions in the automation system (Page 160)"

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

2.9 Reporting batch data

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.

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 O9 "Backup and restore"

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"

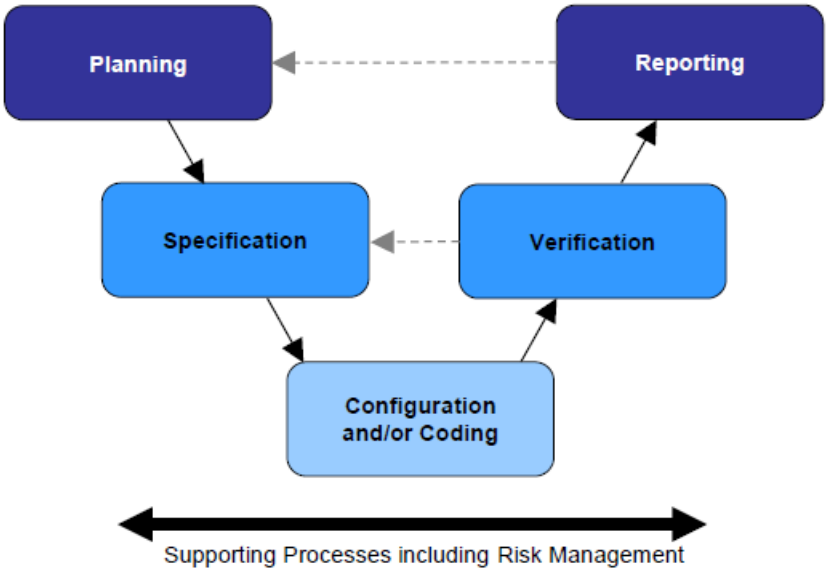
System Specification

3

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) as a response to user requirement specifications (URS)
- System specification general (DCS design, general topics)
- Hardware (and network) design specification (HDS)
- Software design specification (SDS)
- HMI design specification

3.1 Selection and specification of the hardware

Different types of systems are used both for automation and operator control and monitoring of simple and more complex production processes and manufacturing operations.

The choice of hardware components should be appropriate for the requirements. These requirements can be functional in nature, but also include aspects such as local conditions, software compatibility or data security.

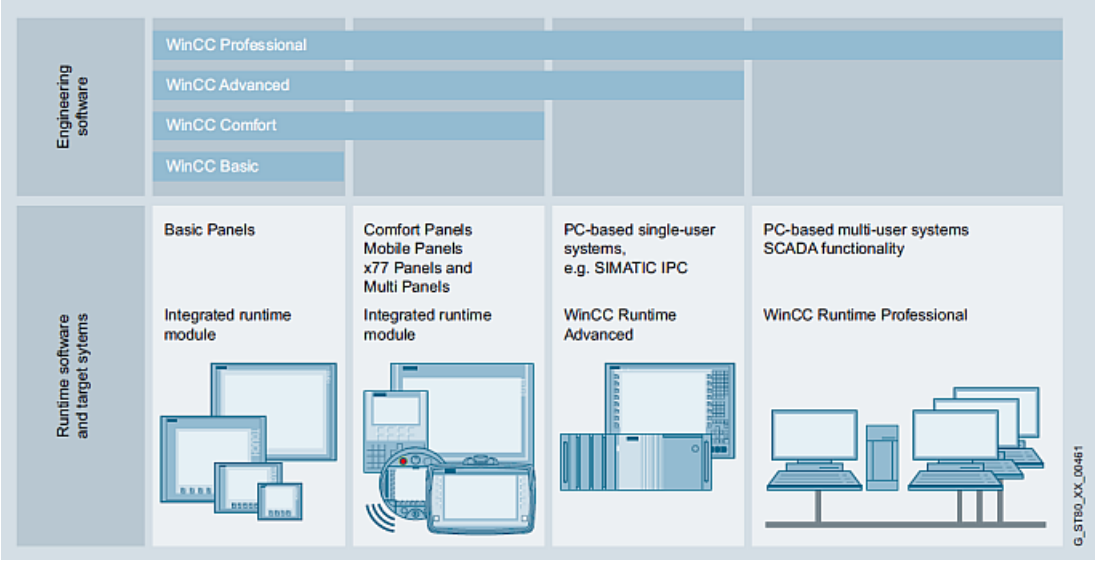
3.1.1 Selection of the hardware components for automation systems

The automation system is selected based on the requirements for the control of the production process. The devices of the SIMATIC S7-1500 series with their display for on-site diagnostics and expanded protection functions are especially well-suited for operation in validated plants. Selection criteria are the processing speed of the program, the program size and available interfaces (Profibus interfaces, Ethernet interfaces, or multiple interfaces). Step sequences can be easily realized with the optional S7 Graph programming language. Special requirements for safety are met through fail-safe devices that automatically bring the plant to a safe state in case of failure.

3.1.2 Selection of the hardware components for HMI devices

For operator control and monitoring of the production process, a selection is made from local HMI devices all the way to multi-station systems with server/client.

- Single-station system with complete operator control and monitoring of a production process through local HMI devices (Comfort Panel or Multi Panel), Panel PC or standard PC
- Multi-station system consisting of operator terminals (WinCC clients) and a WinCC server that supplies the WinCC clients with data



The system availability and data reliability can be increased, especially for PC components with critical functions, by using RAID systems of a suitable class (1, 5) or a redundant system design. With respect to the selection of panels, an Ethernet connection is recommended for backing up the data on a network drive.

The effort for specification and testing is significantly reduced through the use of system-tested hardware components and system configurations.

For specific requirements at the machine level of production plants (for example, in the food and beverage industry or the pharmaceutical industry), Siemens offers extremely rugged panels and Panel PCs with touch screens and stainless steel fronts.

If an HMI device is also intended for operator interventions, the (regulatory!) requirements for recording of these interventions in an audit trail must be taken into consideration when the hardware components are selected.

Note

We recommend the use of released hardware from the current SIMATIC HMI Product Catalog CA 01 because these hardware devices have been system-tested for compatibility by Siemens. See also TIA Selection Tool (https://w3.siemens.com/mcms/topics/en/simatic/tia-selection-tool).

See also

- Functional differences between the SIMATIC Panels, Online Support under entry ID 40227286 (https://support.industry.siemens.com/cs/ww/en/view/40227286)
- Stainless steel housing for SIMATIC HMI Panel PC Ex / Thin Client Ex, Online Support under entry ID 78056495 (https://support.industry.siemens.com/cs/ww/en/view/78056495)

3.1.3 Hardware specification

The hardware (and network) design specification (abbreviated HDS) describes the hardware architecture and configuration. The HDS should, for example, define the points listed below. This is used later as a test basis for the verification.

- Hardware layout plan and network structure
- PC components for server and client including installation procedures
- Automation system with CPUs, I/O cards, field devices, control cabinets, etc.

The HDS can be part of a complete specification or in a separate document.

Note

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

See also

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

3.2 Security of the plant network

In order to meet current customer requirements for networked systems and to ensure the highest possible data security at all times, data and information security is of great importance when establishing networked systems.

Measures for increasing data and plant security

SIMATIC offers several ways to increase data and information security and therefore the security of a production plant. These include:

- Central user administration, staggered user groups and user rights
- Security concepts for network security and restricted access to network drives in an open system
- SIMATIC NET SCALANCE-S firewall and VPN modules
- SIMATIC Security Controller (SSC), in combination with WinCC RT Professional

See also

- Chapter "Data and information security (Page 64)"
- 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", Online Support under entry ID 60119725 (https://support.industry.siemens.com/cs/ww/en/view/60119725)

3.3 Specification of the basic software

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

The components of commercially available standard software include software of third-party providers such as operating systems, Adobe Reader, MS Office, etc.

Note

This software specification is used as an acceptance criterion during subsequent tests (FAT, SAT, etc.), see also chapter "Verification of software (Page 184)".

The SIMATIC WinCC (TIA Portal) software consists of engineering and runtime components for different-sized HMI devices. The corresponding runtime components run on their associated hardware. This is configured and programmed in the engineering interface.

Because the functionalities and applications on on-site HMI devices (panels) differ significantly in some cases from those in a SCADA environment (Supervisory Control and Data Acquisition), the technical functions for WinCC Professional are described in chapter "Configuration for WinCC RT Professional (Page 97)" and the technical functions for WinCC Comfort/Advanced are described in chapter "Configuration for WinCC Comfort / WinCC RT Advanced (Page 127)".

GMP-relevant technical functions for the SIMATIC S7-1500 automation system are presented in chapter "Configuration for SIMATIC S7-1500 Automation Systems (Page 153)" of this manual.

Hardware and software requirements and operating system selection

Information on releases of the various WinCC variants and options with the operating systems (32-bit and 64-bit) can be found in

- Product Catalog CA 01
- In the TIA Selection Tool (https://w3.siemens.com/mcms/topics/en/simatic/tia-selection-tool)
- Compatibility tool (http://www.siemens.com/kompatool)
- Online help, Readme file

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 "Update of the system software (Page 199)".

Basic components of SIMATIC WinCC Comfort / Advanced / Professional

Designation	Brief description	Availability		
		Comf	Adv	Prof
Graphics	Editor for creating graphics	X	X	X
HMI tags	Tag management	X	X	X
User administration	User administration	X	X	X
HMI alarms	Alarm logging	X	X	X
Archives	Process value logging	X	X*	X
Recipes	Creation of recipes	X	X*	X*
Reports	Report creation	X	X	X

Additional SIMATIC components

Designation	Brief description	Availability		
		Comf	Adv	Prof
SIMATIC Logon	Connection to Windows User Management	-	-	X*
SIMATIC Logon Remote Access	Connection of panels to a central user administration with SIMATIC Logon	X*	X*	-
WinCC Audit for SIMATIC Panels / Runtime Advanced	Recording of operator actions	X*	X*	-**
WinCC Server	Servers in a server/client structure	-	-	X*
WinCC Client	Client in a server/client structure	-	-	X*
WinCC Redundancy	Redundant servers			X*
WinCC WebNavigator	View of data and operation of process screens via the web	-	-	X*

Designation	Brief description	Availability		
		Comf	Adv	Prof
WinCC WebUX	Mobile operator control and monitoring via Intranet/Internet	-	-	X*
WinCC DataMonitor	View of data using a browser	-	-	X*
SIMATIC Process Historian	Central long-term archiving of process values and messages	-	-	X*

* = This component requires an additional license

** = Audit trail can be implemented by configuration, see chapter "Audit trail (Page 102)".

Basic components for automation systems

Designation	Brief description
Program blocks	Program structure subdivided into Main, FCs (functions), FBs (function blocks) and data blocks
Technology objects	Configuration of standard controls for PID, counting and measuring, Motion Control
PLC tags	Compilation of digital and analog inputs/outputs
PLC data types	Data structures that are used repeatedly
PLC messages	Messages for chronological messaging
Watch and force tables	Compilation of data for online monitoring during commissioning
Traces	Monitoring and evaluation of process values
Device proxy data	Generation of device proxy files for IPE (Inter Project Engineering)

Additional components for automation system

The S7-PLCSIM software provides the platform for a functional test of the created user blocks, independent of the available target hardware. The software version must be compatible with the version of the engineering system.

3.3.1 Basic software for user administration

An essential requirement – particularly in the GMP environment – is control of access to the system. This is the only way to ensure secure operation in compliance with regulations (US 21 CFR Part 11 and EU GMP Guide Annex 11).

Unauthorized access to the operator control and monitoring system and to the file system and directory structures in the operating system must be prevented. This requires appropriate planning:

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

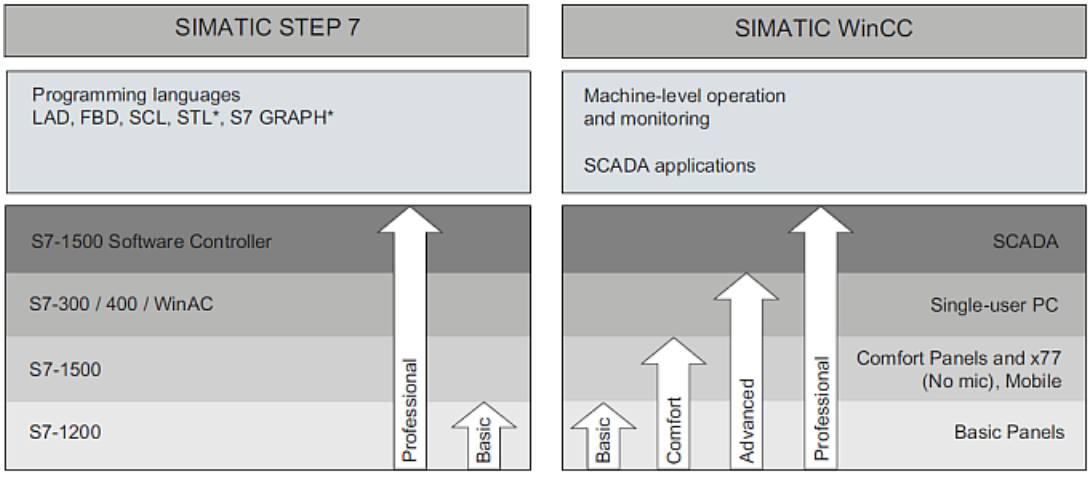
In a single-station system or a distributed system with multiple HMI devices (also in combination with panels), users can be centrally administered on a computer in a workgroup or domain.

SIMATIC Logon supports a user administration based on Windows mechanisms that can be used both in a workgroup and in a Windows domain. Information on the installation and configuration of SIMATIC Logon is contained in the chapter "Setting up the user administration for HMI devices (Page 48)" for HMI devices and in the SIMATIC Logon Configuration Manual.

For local HMI devices without a network connection, the user administration must be set up locally on each panel (see chapter "User administration without SIMATIC Logon (Page 55)").

3.3.2 Basic software engineering

The TIA Portal is the common engineering interface for the automation level and the HMI devices. The S7-1500 automation systems are programmed with the SIMATIC STEP 7 Professional (TIA Portal) engineering system. The WinCC Comfort, WinCC Advanced and WinCC Professional variants are offered for the configuration of HMI devices suitable for the GMP environment. The required variant depends on the type of HMI devices in use, ranging from panels and industrial PCs to standard PCs. The selected variant is added to the STEP 7 engineering system.



The respective WinCC Engineering System contains all the basic functions for engineering the HMI devices. At the center is the project navigator in which all devices belonging to the project are managed. The editors for configuring the different functions are opened for each HMI device from the project navigator. Copy functions simplify the transfer of configured data to other HMI devices.

Tag management

In the TIA Portal, automation systems and HMI devices can be created in a project. Inputs and outputs are maintained in a separate tag table for each controller (PLC). The HMI devices are connected to the process by connecting the external HMI tags to the PLC tags in the PLC tag tables. The TIA Portal creates the integrated connections automatically. For this reason, the tags are maintained only by the PLC. After compilation, corrections are transferred automatically to the project data of the HMI devices. This ensures that tags are maintained consistently throughout the project.

If automation systems and HMI devices are configured in separate TIA projects within the framework of Team Engineering, the project-wide consistency of process tags is brought about by the device proxy files. The tags are also maintained here only in the project data for the automation system.

See also

- Chapter "Inter Project Engineering (IPE) (Page 72)"

Libraries

The project library is used for storing the configured data. Both configured WinCC objects, such as complete graphics, graphics elements, control objects, tags, and scripts, as well as PLC program blocks and PLC data types can be saved in the project library and used multiple times in the project. The global library, in which completely configured devices can also be stored, supports cross-project data storage.

Export / import of project data

The WinCC engineering system has export / import interfaces. Alarms, recipe data records, text lists, tags and project texts can be exported and re-used in another project. An export generates either XLSX or CSV files, which can be edited using the standard Microsoft Excel software and imported back into the project. However, manual documentation of the changes in accordance with the change control procedure must be ensured when importing into an existing project.

Options for the Engineering System

Designation	Brief description
UMC	Central, cross-project user management
Multiuser	Working together on a TIA Portal project
Teamcenter Gateway	Connection to Teamcenter
Cloud Connector	Access to local interfaces using RDP

3.3.3 Basic software for automation level

Hardware configuration, network connections and user program are stored on the local SIMATIC Memory Card of the S7-1500 automation system. After the automation device is started, the compiled user program is processed cyclically and data is exchanged with the I/O devices.

3.3.4 Basic software for operating level

The runtime software (RT) is used for operator control and monitoring of the production process. Functionalities for recording and displaying of runtime data are described in the following.

Alarms

Many 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 end user at the beginning of the project.

Note

The display suppression functionality of the WinCC RT Professional runtime software can be used to suppress the display of selected alarms, for example, during startup phases. The alarms are still recorded in the WinCC alarm log.

For additional information, refer to the TIA Portal Information System > Visualize processes > Working with alarms > Working with alarms > Configuring the output of alarms > Configuring the alarm view (RT Professional) > Configuring alarm display suppression (…)

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

Archives

In the regulated environment, relevant production and quality data must be kept in some cases for 5, 10 or more years. This data must be defined, stored safely and moved to external archives according to data volume or time period. The process, the corresponding data and archive components should be defined for this. See also chapter "Data archiving (Page 34)" and chapter "Electronic data recording and archiving (Page 106)" for WinCC RT Professional or chapter "Electronic data recording and archiving (Page 137)" for WinCC Comfort/Advanced.

The WinCC RT Professional runtime software can also be used to archive process values in compressed form in compressed archives.

Recipes

A system 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. The number of data records and recipes depends on the selected HMI device.

Audit trail

Operational entries and changes to GMP-relevant data must be documented with time stamp, user ID, old value and new value in the form of an audit trail. This can be configured as appropriate for the values involved and is stored in the alarm history (WinCC RT Professional).

Specifically for panels and for the WinCC RT Advanced runtime software, the Audit option fulfills the required functionality of an audit trail, see also chapter "GMP project setting in the Audit option (Page 74)".

Note

To make it easier to view and check GMP-relevant entries, values and changes during plant operation, it makes sense to categorize these already during the specification phase. The process owner should be able to name the GMP-critical values and define them in advance.

3.3.5 Data archiving

Tag values, system messages and audit trail can be archived. The performance scope of the archiving and the method depends on the hardware of the used HMI device and the runtime software.

Archiving for panels and WinCC RT Advanced

The archives are stored on the local system. A memory card is used for local data archiving in the case of panels. By means of a network connection, the archives can be automatically moved or copied to a network drive. Alternatively, panels have USB ports for manual backup. The archive size is dependent on the available memory space.

Archiving with WinCC RT Professional

The basic package of the WinCC RT Professional runtime software contains possible archive configurations for single-station systems and server/client structures. A configuration for the export to a different computer is set in addition to archive size and segment change.

Long-term archiving of process values and messages can be created, for example, with a long-term archive server or with the SIMATIC Process Historian option. The possibilities are described in the chapter "Setting up long-term archiving (Page 48)".

Batch-based archiving

The WinCC Premium Add-on PM-QUALITY is available for batch-oriented acquisition and archiving of production-relevant data such as process values and messages, see WinCC RT Professional chapter "Archiving batch data with PM-QUALITY (Page 110)" or for WinCC Comfort / RT Advanced chapter "Archiving batch data with PM-QUALITY (Page 140)".

Note

The Data Log function of the automation systems provides another easy way of archiving process values. Because this data cannot be protected from manipulation, this function is not suitable in the GMP environment.

3.3.6 Report generation / reporting

Reports of alarms and process values

Messages, recipe data and current process values can be printed out in the form of reports once they have been defined in the report editor. WinCC RT Professional provides further options for reporting, such as the output of archive data in trends or tables.

Depending on the system, output to the printer is managed either in the task scheduler or by print job. A cyclical or event-dependent starting point is specified for this.

Batch-based reporting

The WinCC Premium Add-on PM-QUALITY is available for a batch-based reporting of the archived data, see for WinCC RT Professional, chapter "Batch-based reporting with PM-QUALITY (Page 144)" or for WinCC Comfort / RT Advanced chapter "Batch-based reporting with PM-QUALITY (Page 112)".

3.3.7 Increase of availability with WinCC RT Professional

The parallel archiving of the relevant process values, alarms and recipes increases the availability of the data. With the "SIMATIC WinCC Redundancy for RT Professional" option, one WinCC system can be operated as a master and another WinCC system as a standby server. The archive data is continuously synchronized. When one system fails, the other system continues the archiving function. As soon as both systems are back online, an automatic data synchronization is performed.

For correct operation of the redundant WinCC system and consistent data display, the WinCC clients should always be connected to the master.

See also

- Chapter "Recording and archiving (Page 108)"

3.4 Specification of the application software

Besides the definition of the hardware (see chapter "Selection and specification of the hardware (Page 25)") and the standard software components (see chapter "Specification of the basic software (Page 28)"), the specification of the application software is an essential part of the design specification. This is used later as an acceptance criterion for the system verification (FAT, SAT, etc.) in addition to the functional specification.

The design specification may consist of one or more documents. Other separate documents are also frequently maintained, for example, process tag list, I/O list, parameter list, P&ID, etc. The status of these documents (version, release) must be defined just as clearly as the other specification documents (URS, FS, DS).

See also

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

For example, the design specification can be divided as follows:

System specification (general)

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

HMI design specification

The following aspects, among others, are specified for the user interface:

- Screen layout and navigation
- Plant screens, unit screens, detailed screens
- Operating level, possibly access authorizations
- Screen hierarchy
- Screen resolution, screen cycles
- Block icons, used graphic elements
- Alarm classes, priorities, alarm numbering ranges, display

Software design specification

- General information such as project name, libraries, plant hierarchy
- Template and module specification, optionally in a separate document
- Reaction to power failure and restart

- Time synchronization, specification of master and slaves
- Description of exceptional conditions for safe plant operation
- Emergency stop characteristics

3.5 Additional SIMATIC software for the operating level

3.5.1 WinCC Premium Add-ons

This manual presents the following WinCC Premium Add-ons:

Designation	Brief description	Availability		
		Comf	Adv	Prof
PM-CONTROL	Recipe data management and job scheduling	X*	X	X
PM-QUALITY	Batch-based data acquisition and reporting	X*	X	X
PM-OPEN IMPORT	Importing of process data	X*	X	X
PM-ANALYZE	Evaluating and analyzing of alarm logs	X*	X	X
PM-LOGON	User logon with RFID card (company ID) via a card reader	X*	X	X

* For data exchange, an Ethernet connection can be used to connect panels to the Premium Add-ons installed on a separate PC.

The WinCC Premium Add-ons are enabled with separate licenses.

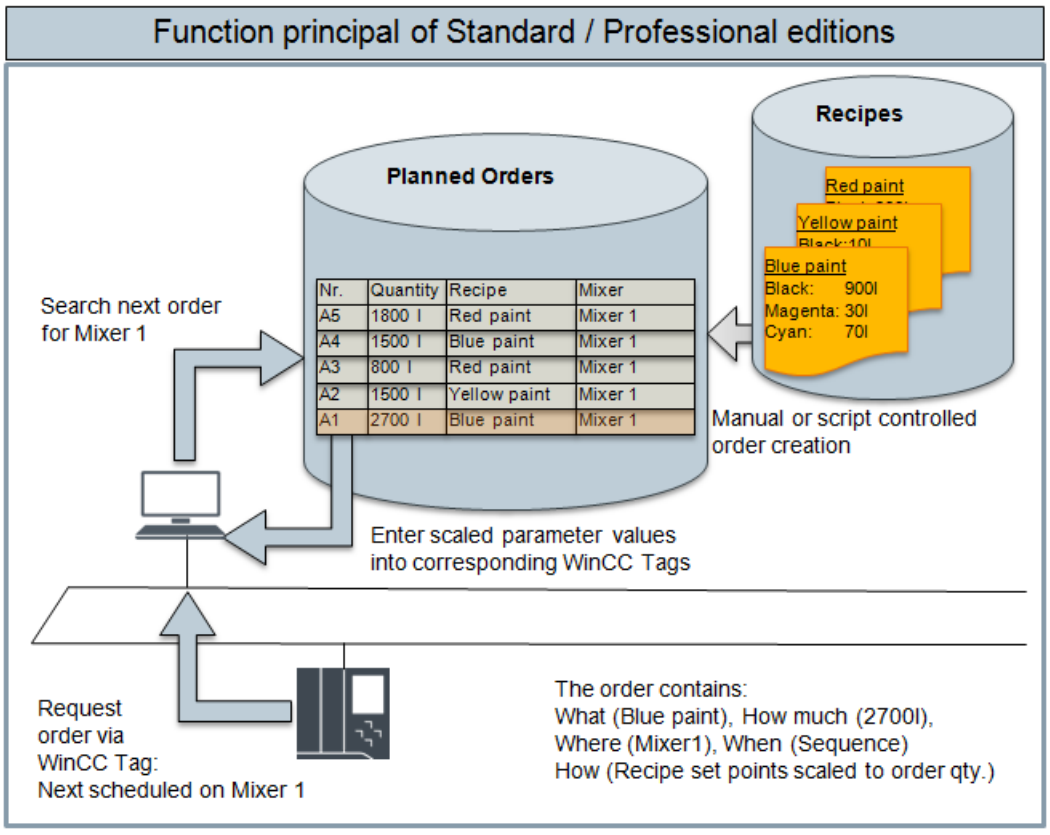
Batch-based control with PM-CONTROL

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 time of production can be specified.

The software package is divided into three applications:

- Topology manager for mapping the plant topology, creating the required parameters and configuring the connection to the automation level
- Recipe system for creating and managing recipes / products with automatic versioning
- Order planning and order control, scheduling and management of production orders

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



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

Batch-based reporting with PM-QUALITY

The data recorded in WinCC Premium Add-on PM-QUALITY can be displayed in curve diagrams, printed out on a printer in report form or exported via an HTML or 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, messages and operator interventions
- Report Editor for the individual creation of report layouts to show the acquired batch data in reports and to display it on the screen
- Data Logging, runtime component for acquiring data
- Data View and various ActiveX controls for displaying the batch data
- Data Center for merging the batch data acquired in parallel in redundant systems

Besides 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 reports by the logged-on user and with it the manual assignment of the batch status (released / locked).

If the released batch report has been exported automatically due to the export option setting, no more changes can be made to the report if the "complete automatically" property is selected.

Batch-based archiving with PM-QUALITY

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

Importing archives with PM-OPEN IMPORT

With PM-OPEN IMPORT, process data (tag and alarm logs) and operator actions (audit trail), which are logged by panels and HMI devices with WinCC RT Advanced in CSV format, are transferred to the WinCC RT Professional databases. 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 WinCC Runtime are used for viewing the data.

Evaluating and analyzing archives with PM-ANALYZE

PM-ANALYZE assists in 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 data archives of the PM SERVER. These archives form the database for the evaluations and analysis functions in PM-ANALYZE. Convenient filter settings for filtering messages by message content and time range, as well as statistical analyzes by volume and frequency, reveal defects and weak points. With dotted, step or curve lines as well as bar and pie charts, PM-ANALYZE has a wide range of charts for displaying the archived process values. The special feature of PM-ANALYZE is the parallel display of charts and messages in a workspace. Interrupts in tables and statistical evaluations parallel to process values in charts show the spectrum of production data at a glance, even with large amounts of data.

3.5.2 Interfaces to process data

WinCC WebNavigator

Remote access to the WinCC project data is set up with the WinCC WebNavigator option in combination with the WinCC RT Professional runtime software. To view the process screens, users with the necessary rights must authenticate themselves using their password. The details are checked by SIMATIC Logon. Operation of the process screens is subject to access control, which is defined in the WinCC project in the user administration.

See also

- Chapter "Setting up a web connection (Page 117)".

WinCC WebUX

The WinCC WebUX option provides a device- and browser-independent remote access to the WinCC project data. The display and operation of the process screens is subject to restrictions. Remote operation depends on the access control defined in the WinCC project in the user management. An authorized user must authenticate with password. The details are checked by SIMATIC Logon.

WinCC DataMonitor

WinCC Data Monitor is a dedicated display and analysis system for process data from WinCC and data from the WinCC long-term archive server. WinCC DataMonitor provides a number of analysis tools for interactive data display and analysis of current process values and historical data:

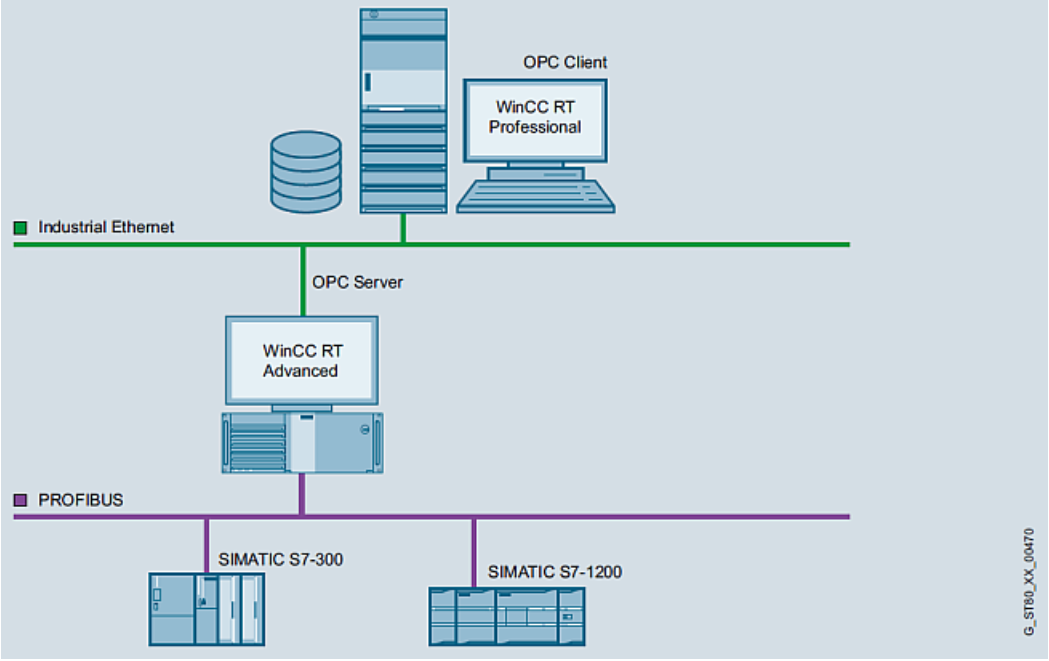
- Excel workbooks
- Published reports
- Trends and alarms
- Process screens
- Web center

3.5.3 Connection to host systems

The options for connection to host systems depend on the HMI device used.

Interfaces of panels and single-station systems with WinCC RT Advanced

Process values for visualization and archiving can be provided to an OPC client in a data communication based on OPC (OLE for process control). For this purpose, panels can be configured as OPC UA servers and single-station systems with WinCC Advanced as OPC DA (DCOM) or OPC UA servers.



Interfaces of the SCADA system to host systems

Standardized access with OPC and OLE DB from computer systems of the plant management level to computer systems of the process level is integrated in WinCC Professional. WinCC Professional provides access to the following process data:

- Interrupts and events (alarms), OPC A&E, read and write (acknowledgments only) access
- Process value logs (trends), OPC HDA, read and write access
- Process tags (states), OPC DA, read and write access,
- Data communication via DCOM
- Process tags, OPC XML DA, read and write access via web service
- Process values and process value archives, OPC UA (Unified Architecture), read and write access
  The data exchange is based on the TCP/IP protocol with exchange of digital certificates.
- All archive data, WinCC OLE DB, read-only access

3.6 Utilities and drivers

3.6.1 Printer drivers

For panel PCs and standard PCs, we recommend using the printer drivers integrated in the operating system and released for WinCC. No guarantee for proper operation of the system is made if external drivers are used.

Printout from local printers or network printers is possible for panels. Hard copies or reports can be printed on a network printer. Line printing of alarms is only possible on a local printer.

A list of the released printers and the required settings for the panels are compiled in the product support at:

- "Printers for SIMATIC HMI Panels", Online Support under entry ID 11376409 (https://support.industry.siemens.com/cs/ww/en/view/11376409)

3.6.2 Virus scanner

The use of virus scanners on panel PCs and standard PCs is enabled during process mode. The released virus scanners can be accessed via the compatibility tool (http://www.siemens.com/kompatool) in the product support.

The following settings must be observed when using virus scanners:

- The real-time search is one of the most important functions. However, it is sufficient to examine the incoming data traffic.
- Scheduled scans must be disabled because they restrict the performance of the system considerably during process operation.
- Manual search must not be performed during the process operation. It can be performed at regular intervals, for example, during maintenance intervals.

These arrangements should be defined in the specification and/or optionally in a work instruction 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. A quick restoration of the system is possible with the system and user software backed up in the image. Backed up hard drive contents can also be imported to devices of the same type. This facilitates the process of replacing computers.

The "SIMATIC Image and Partition Creator (IPC)" provided by Siemens is a software package that can be used to accomplish these tasks. This is also possible without a separate installation

through direct use from CD or USB FlashDrive. Administration skills are needed for this process.

Note

The created images are used for restoring the installed system, but are not used for backing up online data.

System Installation and Basic Configuration 4

SIMATIC TIA Portal is a common engineering interface for the automation level, HMI devices and drives.

SIMATIC WinCC (TIA Portal) consists of the engineering software and runtime software for the respective HMI devices. SIMATIC STEP 7 Professional (TIA Portal) contains the engineering system for programming automation systems in all performance classes. Together, the two software packages cover the engineering for the complete portfolio of the automation level and HMI devices.

Different software packages are offered depending on the performance range:

Engineering software for automation level

- STEP 7 Basic (for S7-1200 only)
- STEP 7 Professional

Engineering software for HMI devices

- WinCC Basic for Basic Panels (Audit option is not available)
- WinCC Comfort for all panels
- WinCC Advanced for panels and also for single-station PC systems
- WinCC Professional also for multi-station systems with server-client structure

Runtime software for HMI devices

The respective runtime software is required for the visualization on each HMI device:

- Integrated runtime module for the panels
- WinCC RT Advanced for Panel PC and standard PC
- WinCC RT Professional for complex plants and client-server systems

The runtime software is activated with a license key except for the panels.

4.1 Installation of the operating system

Control panels come preinstalled with the Microsoft Windows CE operating system and the corresponding runtime software.

Note

If the installed Microsoft Windows CE version of the panel does not match the version of the project data, the engineering system has updates for the operating system in store.

For additional information, refer to the TIA Portal Information System > Visualize processes > Compiling and loading > Servicing the HMI device > Updating 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 considered when using standard PCs.

Details can be found in the current product catalog CA 01 or via the TIA Selection Tool (https://w3.siemens.com/mcms/topics/en/simatic/tia-selection-tool).

Current information on the operating system installation can be found in the "Installation" chapter of the TIA Portal Information System.

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. Prohibited characters are listed in the TIA Portal Information System under Installation> System requirements for the installation > Product-specific features.

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

4.2 Installation of SIMATIC components

4.2.1 Installation of the engineering software

The SIMATIC STEP 7 (TIA Portal) and SIMATIC WinCC (TIA Portal) engineering software are installed on a SIMATIC PG / PC or a standard PC and set up the TIA Portal. The software is activated in each case with licenses. The license for the HMI devices determines the corresponding variant.

The TIA Portal acts as a central engineering interface. Project data is created for the automation systems and for one or more HMI devices of different types. After compilation, the

project data is transferred to the respective automation system or the corresponding HMI device. The project can be started on the device for the current production.

Note

Please note the installation sequence. First, the engineering software SIMATIC STEP 7 Professional (TIA Portal) is installed and then the engineering software SIMATIC WinCC (TIA Portal) in the selected version.

4.2.2 Installation of the SIMATIC WinCC RT runtime software

Panels and panel PCs are available as complete systems with pre-installed and licensed WinCC RT.

WinCC RT must be installed and licensed separately on each operator control and monitoring component for server/client systems or standard PCs.

Additional licenses are required for any other options that are used.

Note

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

SIMATIC Security Controller

During installation of the WinCC RT Advanced and WinCC RT Professional runtime software, default settings in the Windows operating system are automatically adapted to the requirements of the software. The required settings in the operating system are managed in the SIMATIC Security Controller application for WinCC RT Professional. The application can be opened after installation using Start > Programs > Siemens Automation > Security Controllers, and the settings made can be viewed there. An option for saving and printing is provided.

The following settings are configured automatically for specific functions:

- Required Windows user groups
- Security-related registry entries
- Configuration of the Windows firewall exceptions list
- DCOM settings (Distributed Component Object Model), for WinCC RT Professional only
- 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 joined to a different work environment (domain or workgroup), the settings must be re-configured by SIMATIC Security Controller.

See also

- TIA Portal Information System > Installation > Notes on the installation

4.2.3 Options for SIMATIC WinCC (TIA Portal)

The options for the HMI devices can be configured in the engineering software without the need for an additional license. The license is required on the respective HMI device so that the configured option is operational.

Licenses are supplied on USB sticks or as download and transferred to the HMI device using the "Automation License Manager" tool. For panels, the license is transferred via the engineering system, the Automation License Manager or ProSave. The procedure is described in the TIA Portal Information System.

The WinCC Premium Add-ons described here are installed after the WinCC runtime software and licensed with using a USB dongle or software license.

4.2.4 Setting up long-term archiving

For long-term archiving of process value, alarm and audit trail logs, the log data can be moved to a network drive or outsourced to another computer. The required (and only the required!) access authorizations must be set up for this.

The task scheduler or an event for copying or moving the logs can be configured for panels and HMI devices with WinCC RT Advanced, see chapter "Electronic data recording and archiving (Page 137)".

For HMI devices with WinCC RT Professional, long-term archiving can be created with the long-term archive server or the WinCC option SIMATIC Process Historian, see also chapter "Electronic data recording and archiving (Page 106)".

4.3 Setting up the user administration for HMI devices

For secure operation that is compliant with regulations, controlled access to both the operating level and configuration level and to archives and backup copies is required. A user-based logon and logout for operator actions is one of the basic functionalities for meeting this requirement.

To organize the operator authorization, users are assigned to different user groups according to their tasks. Authorizations for the individual operator actions are assigned to each user group in the project data for each HMI device.

Note

The structure and the authorizations 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 engineering phase.

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

All authorizations for operator control elements on the visualization interface (faceplates, input fields, buttons etc.) must be set up according to the specifications.

Note

For distributed systems (also in combination with panels) or single-station systems with WinCC RT Professional, we recommend implementation of user administration based on SIMATIC Logon and Microsoft Windows Administration.

The user administration is set up locally for local HMI devices without a network connection. Users and their user group assignment are then only known locally.

4.3.1 User administration with SIMATIC Logon

User administration with SIMATIC Logon is based on the mechanisms of the Windows operating system. The users and groups are configured according to the specification in the user administration of Windows.

The following steps must be performed when setting up the user administration based on SIMATIC Logon.

- Setup of the user groups and users in Windows
- Installation and setup of SIMATIC Logon
- Setup of the security settings in Windows (see chapter "Security settings in Windows (Page 50)")
- Administration of the user rights for the respective HMI device

The access control for the operator interface is then configured:

- Assignment of authorizations in the visualization interface (input boxes, buttons, screen windows)
- Setup of access rights in PM-CONTROL or PM-QUALITY if the WinCC Premium Add-ons are used

Both Windows user administration options are always available for this, that is, in a domain or in a workgroup with a central logon server.

See also

- Operating system help of Microsoft Windows or the appropriate Windows manual (for setting up Windows workgroups or a domain)
- TIA Portal Information System > Visualize processes> Configuring user administration
- WinCC Process Visualization System, WinCC Security Concept, chapter 4 "User and access management in WinCC and integration into Windows Management", Online Support under entry ID 23721796 (https://support.industry.siemens.com/cs/ww/en/view/23721796)
- Chapter 6.4.1 in "Security Concept PCS 7 and WinCC" manual, Online Support under entry ID 60119725 (https://support.industry.siemens.com/cs/ww/en/view/60119725)

Windows domain

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

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

All user data is created and managed on the server of a workgroup. SIMATIC Logon checks the logon data against the user administration on this server and provides the logon information to the other computers in the workgroup.

4.3.2 Security settings in Windows

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

- Password policies such as complexity, password length, password age
- Account lockout policies
- Audit policies

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

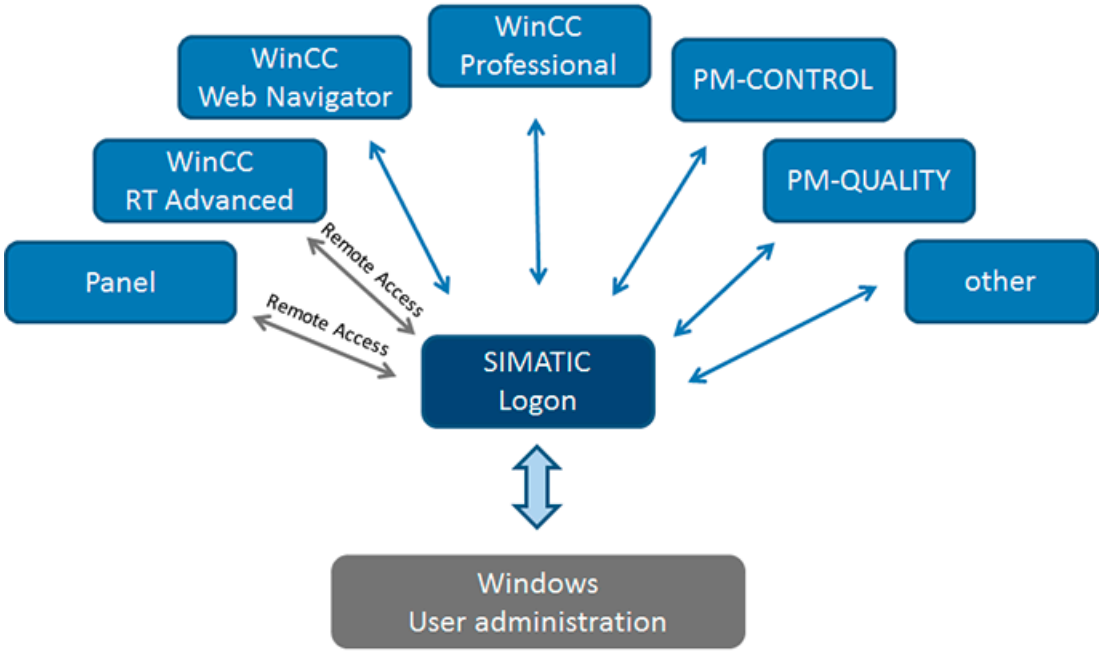
- Chapter "Blocking the operating system level during operation (Page 62)"
- Chapter 7.4 "Password policies" in "PCS 7 Compendium Part F – Industrial Security", Online Support under entry ID 109756871 (https://support.industry.siemens.com/cs/ww/en/view/109756871)

4.3.3 Configuration of SIMATIC Logon

SIMATIC Logon checks the correctness of the logon data of a user on the computer against the central user administration and returns the logon information to the respective HMI device. User logon for the operation of WinCC options and Premium Add-ons can be included in the check by SIMATIC Logon.

Note

If the logon server is unavailable due to a network interruption, the local user administration becomes active instead of the central user administration. In order to bring the plant to a safe state in the event of an emergency, a local user and a local user group with limited operating rights should be created for this.



Note

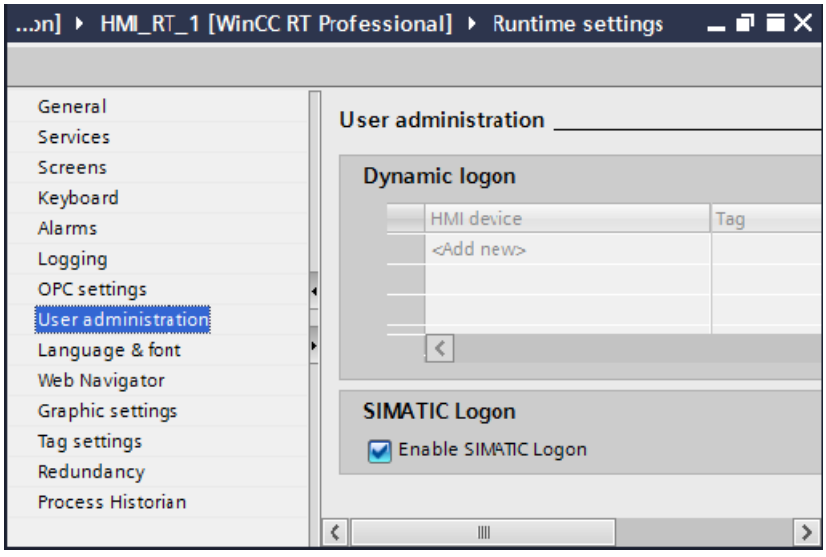
Events such as successful and failed logon/logoffs are stored in the EventLog database of SIMATIC Logon and in the WinCC alarm system.

See also

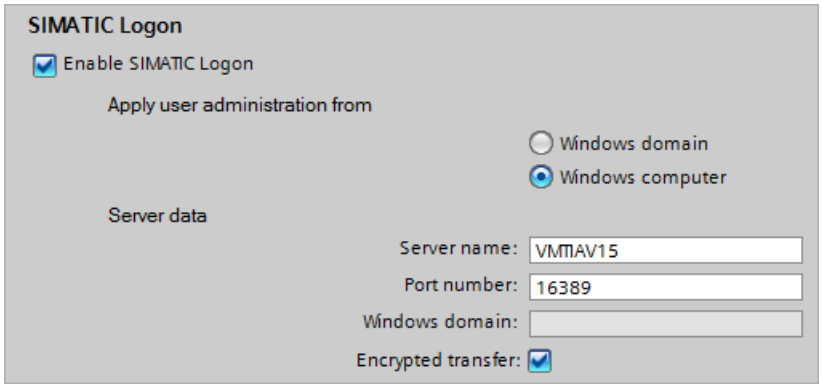
- Chapter "Administration of user rights (Page 57)"
- Chapter 6.4.3 in "Security Concept PCS 7 and WinCC" manual, Online Support under entry ID 60119725 (https://support.industry.siemens.com/cs/ww/en/view/60119725)

The use of SIMATIC Logon is activated in Runtime settings > User administration.

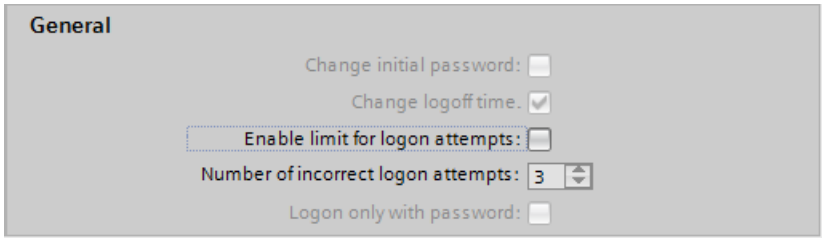
Activation for HMI devices of type WinCC RT Professional



Activation for HMI devices of type WinCC RT Advanced or Comfort Panels

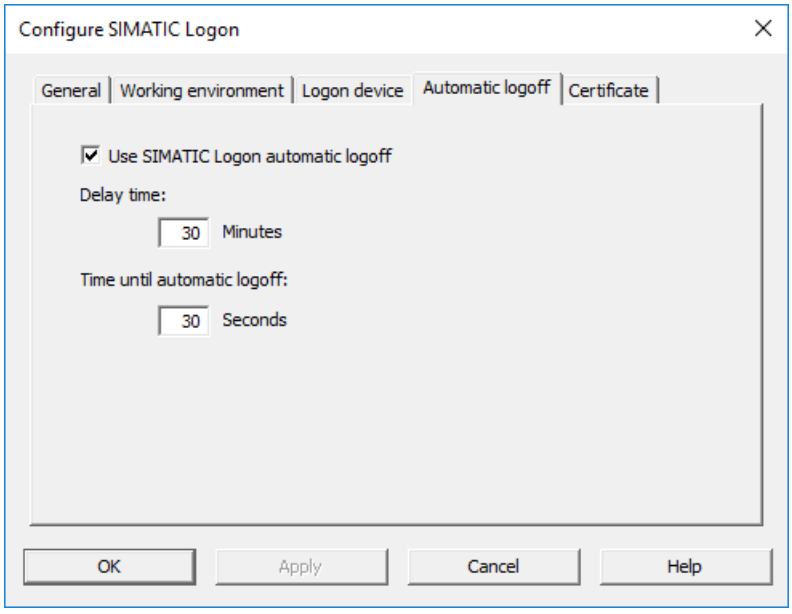


In addition to the user logon via SIMATIC Logon, the number of invalid logon attempts can be limited for these HMI devices.



The initial settings of SIMATIC Logon are made in the "Configure SIMATIC Logon" dialog box. The settings are described in the SIMATIC Logon Configuration Manual and include, for example:

- The logon of a "default user" after user logoff
- Logon server ("working environment")
- Automatic logoff with SIMATIC Logon
- Certificate specification for a TLS-secured connection to HMI devices of the RT Advanced or Comfort Panel type



See also

- Encrypting the connection between SIMATIC Logon and WinCC Comfort / Advanced, Online Support in entry ID 109480490 (https://support.industry.siemens.com/cs/ww/en/view/109480490)

Note

No "auto-logoff" may be activated at the operating system level, otherwise the user interface will be completely closed.

Furthermore, the activation of a screen saver in combination with SIMATIC Logon is not allowed.

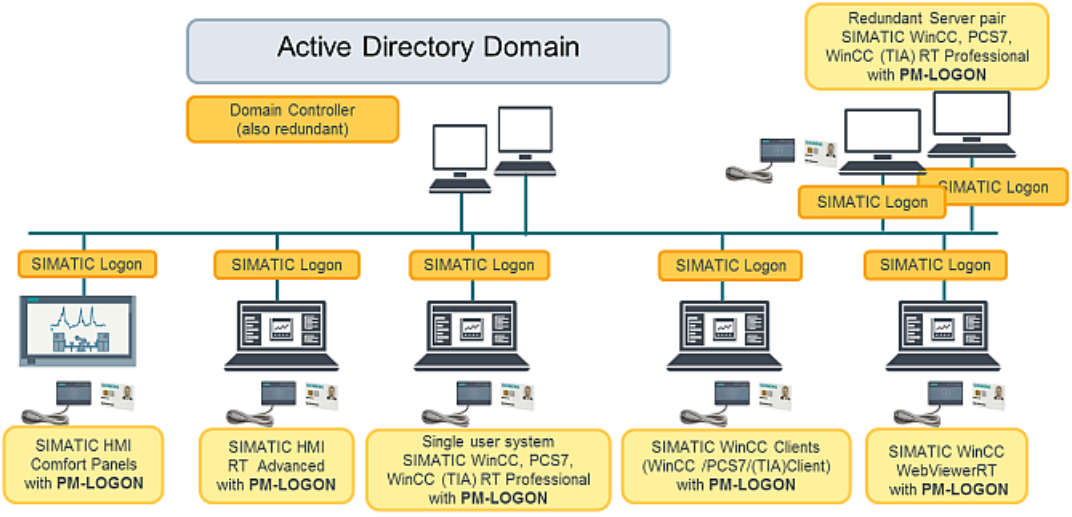
4.3.4 Logon via RFID card reader with PM-LOGON

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

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

The users and user groups are maintained in the Active Directory of a domain or in a Windows workgroup. The ID of the ID card is stored with the user together with the encrypted password. Reading the ID card on the card reader starts a data query via SIMATIC Logon. This provides the user name with which the PM-LOGON Runtime logs the user onto the HMI device.

The application supports various card readers. The card readers are not included in the scope of delivery.

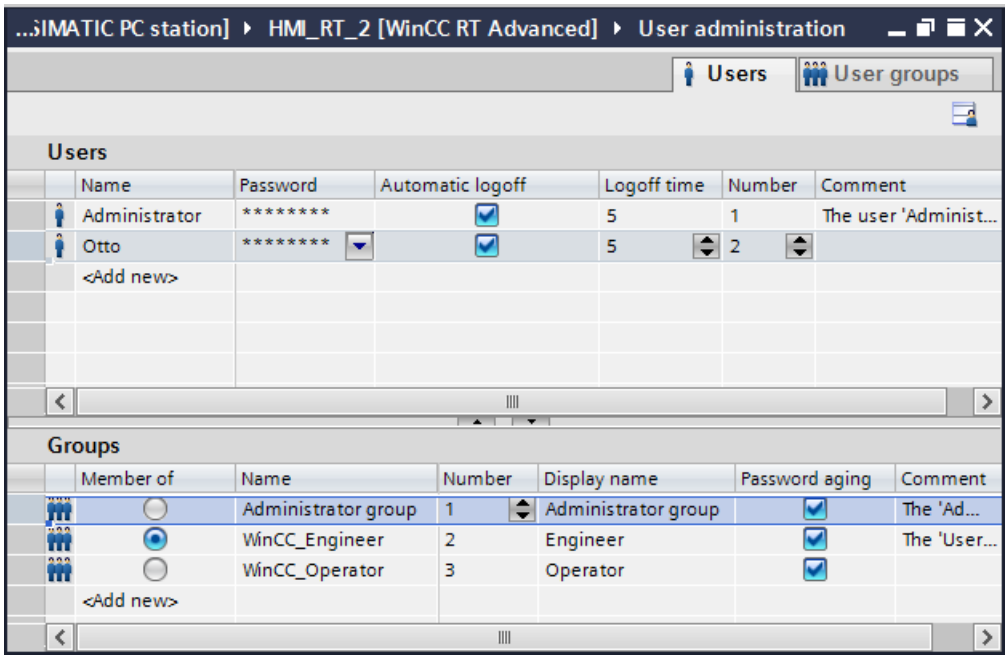


See also

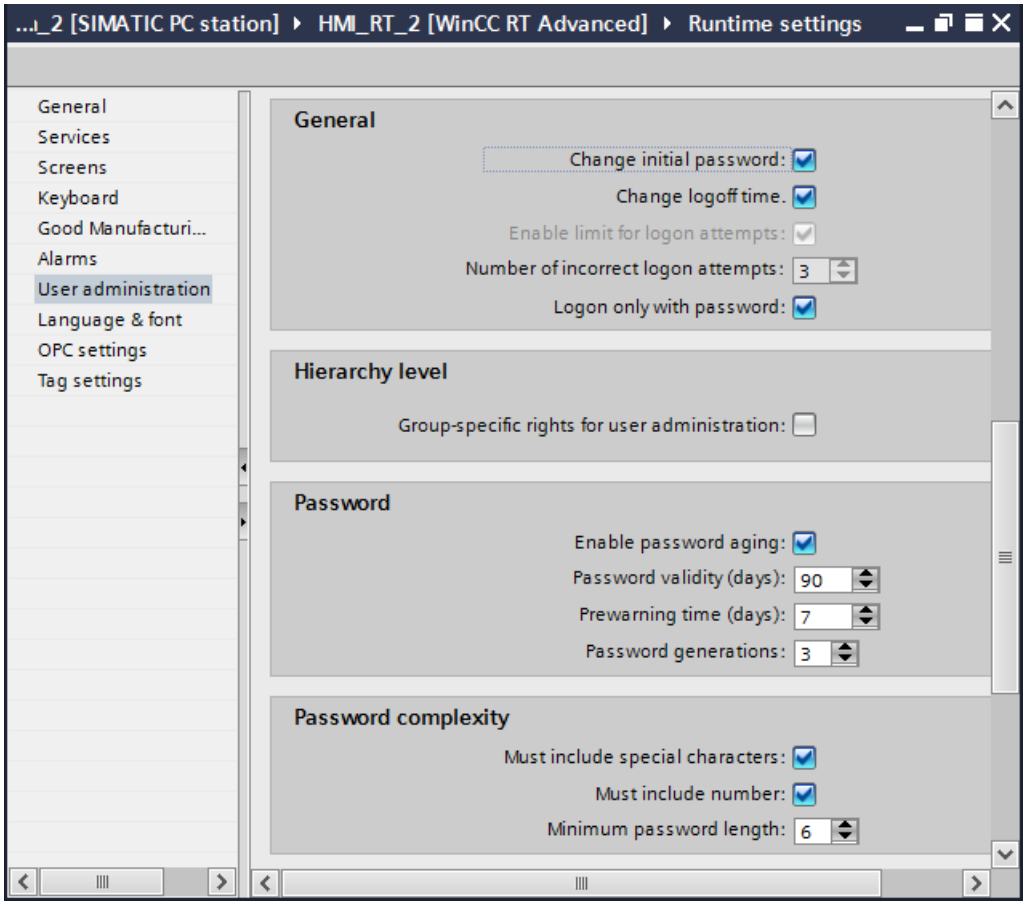
- Information about PM-LOGON under (www.siemens.com\Process-Management)

4.3.5 User administration without SIMATIC Logon

For panels or single-station systems (WinCC RT Advanced), the users and user groups are administered locally. The requirements for access control are met through appropriate configuration.



The password settings, such as password, account lockout and audit policies, are then defined in the local user administration of the HMI device.



4.3.6 Local SIMATIC user groups

The TIA Portal uses the Windows authorization model. During the software installation, various user groups are created beginning with the name SIMATIC in the Windows operating system. These must not be deleted.

For engineering in the TIA Portal and for operating the WinCC user interface, the user logged on to the Windows operating system should not have administrator rights, but only user rights. In process mode, this ensures that only the WinCC RT Professional system software has access to the database.

WinCC Professional automatically manages the security settings and share permissions for the project data. The access rights for the operator interface conform to the configuration in the WinCC user administration and are checked by the respective runtime software, see chapter "Administration of user rights (Page 57)".

See also

- WinCC Runtime Professional Readme > Runtime
- Chapter "Security settings in Windows (Page 50)" applies here as well

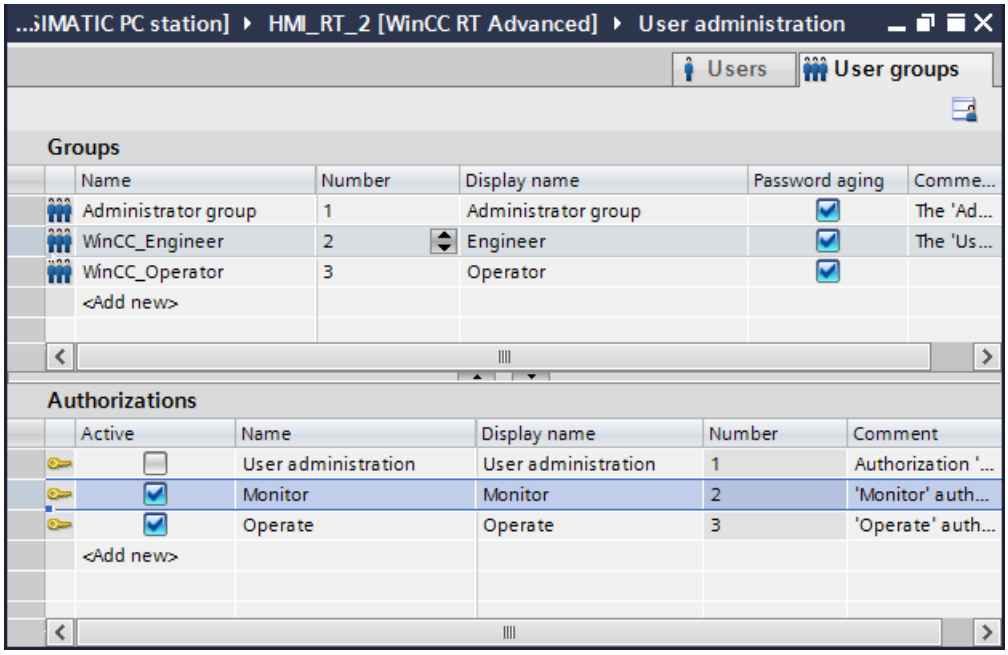
4.4 Administration of user rights

Regardless of whether user administration with SIMATIC Logon or local user administration for a single-station system (panel or RT Advanced) without SIMATIC Logon is used, the user rights for operator input in runtime are defined in the project data of the HMI device.

The user rights are generally assigned to the user groups. The required user groups are created in the project data for this purpose. If SIMATIC Logon is used, the user groups must have the same names as the user groups in Windows.

The following procedure must be followed for this:

- Open the project data for the HMI device in the TIA Portal (engineering system)
- Open the user administration with the "Users groups" tab
- Create group(s)
- Assign rights for each group



The user rights are assigned for the group members using the WinCC user groups in the project data. Members of the "WinCC_Engineer" group, for example, are then assigned the corresponding rights for operator input in the WinCC operator interface.

4.5 Access control for configuration data

4.5.1 Access control for TIA Portal project data

The TIA Portal offers a project-related user administration to protect the project data against unintentional or unauthorized access. Once the project protection has been activated, the project can only be opened or edited by the authorized users. The activation cannot be canceled.

The users can be maintained as project-related users for a TIA Portal project or with the option UMC (User Management Component) as global users and user groups for several TIA Portal projects. Each user is created with user name, password and authentication method.

The TIA Portal provides the following roles, additional roles can be added:

- Open the project read-only
- Open the project with write rights
- Manage users and roles

Project-related user management is also available with the Multiuser Engineering option.

4.5.2 Access protection for automation system

To protect the program data, parameter settings and start/stop of the user program against unauthorized access, the SIMATIC S7-300/400/1500 automation systems provide staggered protection levels for controlled communication. In addition, SIMATIC S7-1500 provides an additional protection level for the connecting to HMI devices and a display protection for operator interventions on-site.

See also

- Chapter "Protection functions in the automation system (Page 160)"
- Chapter "Configuration control (Page 190)"

4.6 Access control at the operating system level

Access to the Windows operating system level is not required and usually not desired for the plant operator registered in the WinCC user interface. Therefore, additional configuration settings (startup behavior, change to the operating system level) must be carried out. These settings prevent unauthorized access from process operation of SIMATIC WinCC RT Professional to sensitive data of the operating system.

Note

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

4.6.1 Startup characteristics

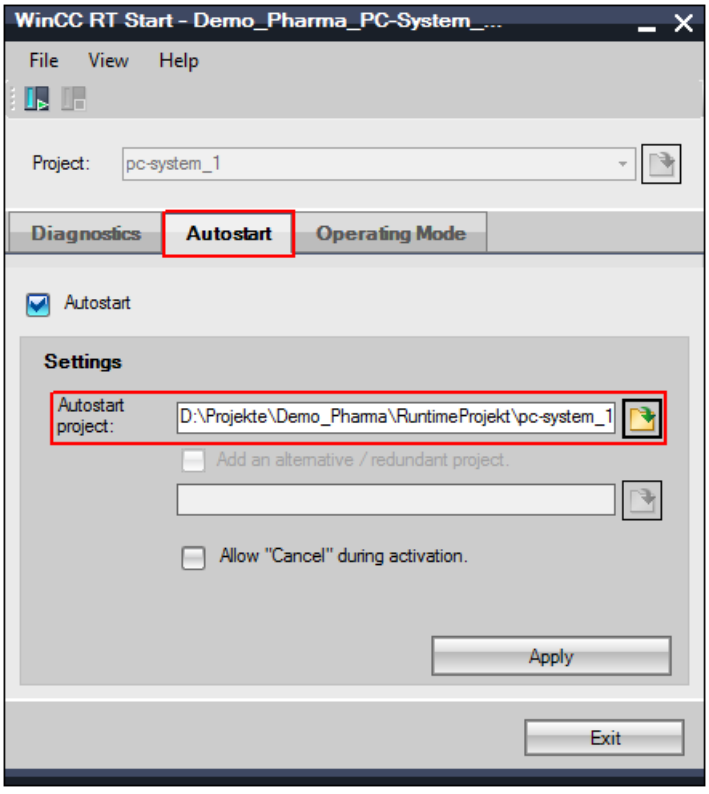
For the safe start of the HMI device, an automatic startup through to the activation of the user interface is configured. In this way, access to the operating system level is prevented during the startup.

Automatic logon in the Windows operating system is described in the Online Support under entry ID 23598260 (https://support.industry.siemens.com/cs/ww/en/view/23598260) in an example for SIMATIC IPCs.

The configuration of the automatic start of the user interface is different for each of the various HMI devices.

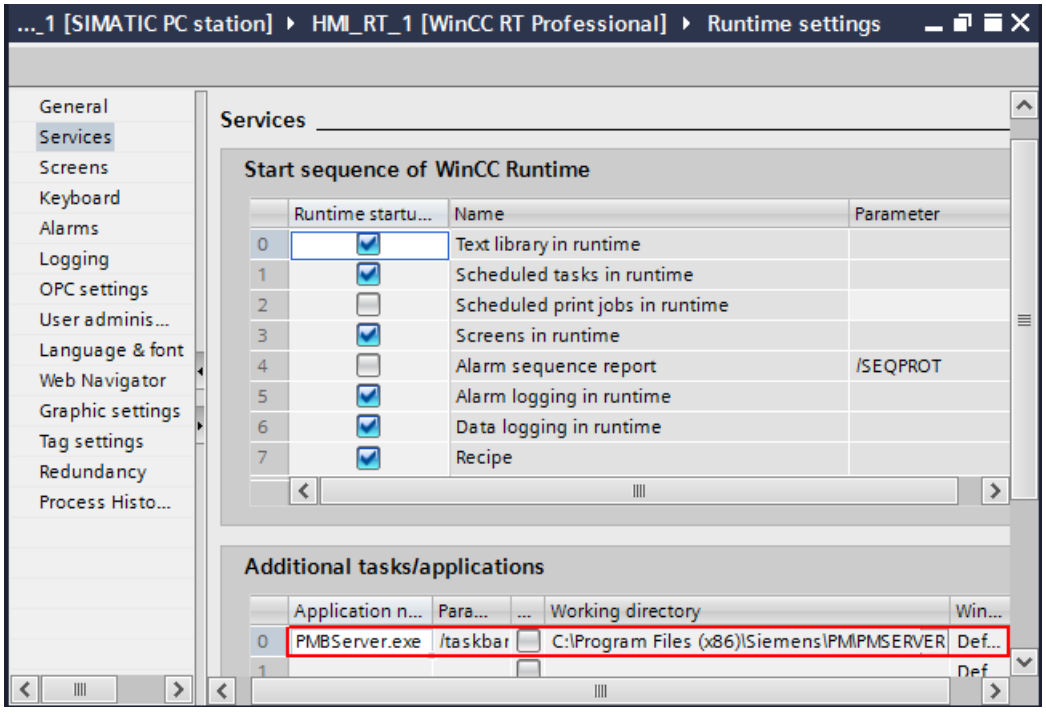
Automatic startup for HMI devices with WinCC RT Professional

The automatic startup is organized in the WinCC RT Start application. This is opened via "Start > Siemens Automation> WinCC Runtime Start".



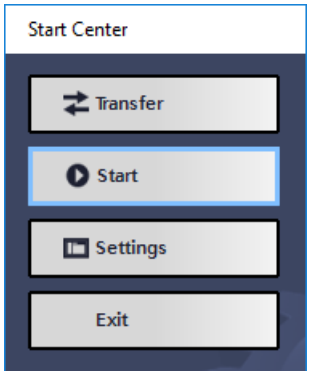
When the "Autostart" property is selected, the specified project is activated automatically when the computer boots up. The "Allow "Cancel" during activation" check box should not be selected, so that the project start cannot be interrupted.

Those editors that will be required during the ongoing operation are selected in "Runtime settings > Services". Other applications that should be started automatically, such as the help application PM-SERVER for the Premium Add-ons PM-CONTROL or PM-QUALITY, are added under "Additional tasks/applications".

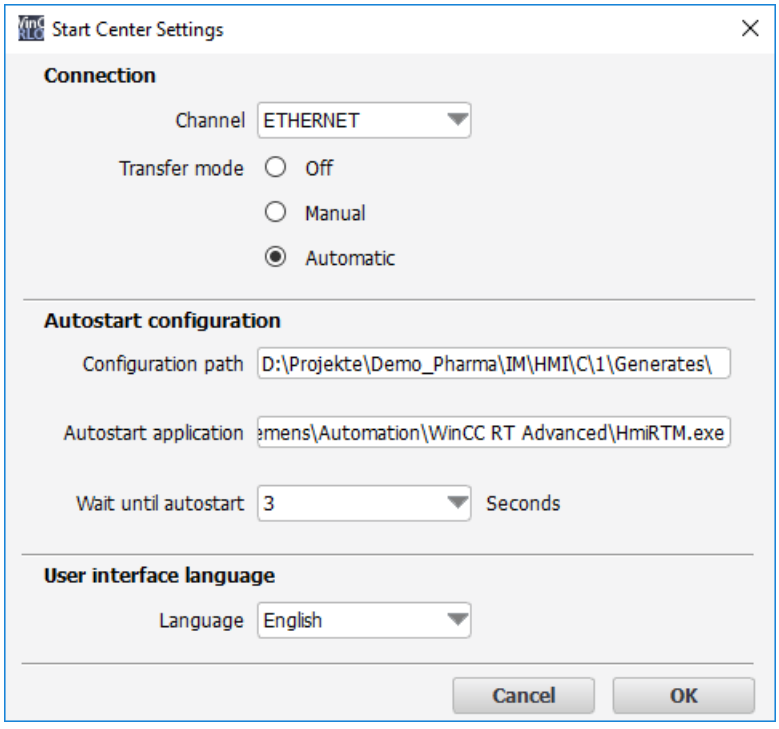


Automatic startup for HMI devices with WinCC RT Advanced

The automatic startup is organized in the Start Center application. This is opened via "Start > Siemens Automation> WinCC Runtime Loader".



The project with project path that is to be started automatically is specified under "Settings". The automatic start of the project data after startup of the operating system is delayed for the number of seconds indicated in the "Wait time" box.



A shortcut to the application StartCenter.exe (C:\Program Files (x86)\Siemens\Automation \WinCC RT Advanced) then has to be set in the Autostart mode of the operating system.

Automatic startup for panels

When the panel is started up, the Start Center is started automatically. The project data is activated after the set time delay. The delay time can be configured in the Control Panel under Transfer> Directories. We recommend setting the value equal to 0, so that the project data is activated immediately.

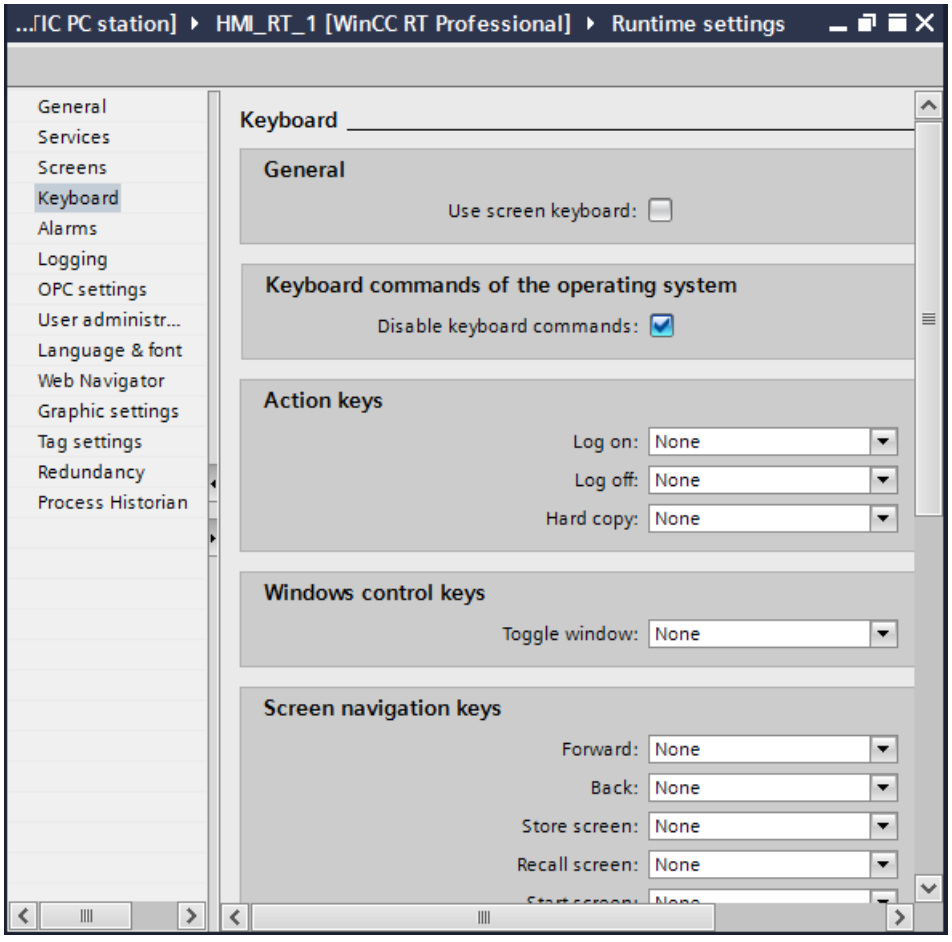
Note

After commissioning, the "Remote Control" property in the Control Panel under "Transfer" should be disabled so that accidental automatic transfer from the engineering system is prevented.

4.6.2 Blocking the operating system level during operation

Configuration settings in WinCC RT Professional

To prevent access to the operating system during process operation, the Windows keys are disabled under "Keyboard" in the runtime settings.

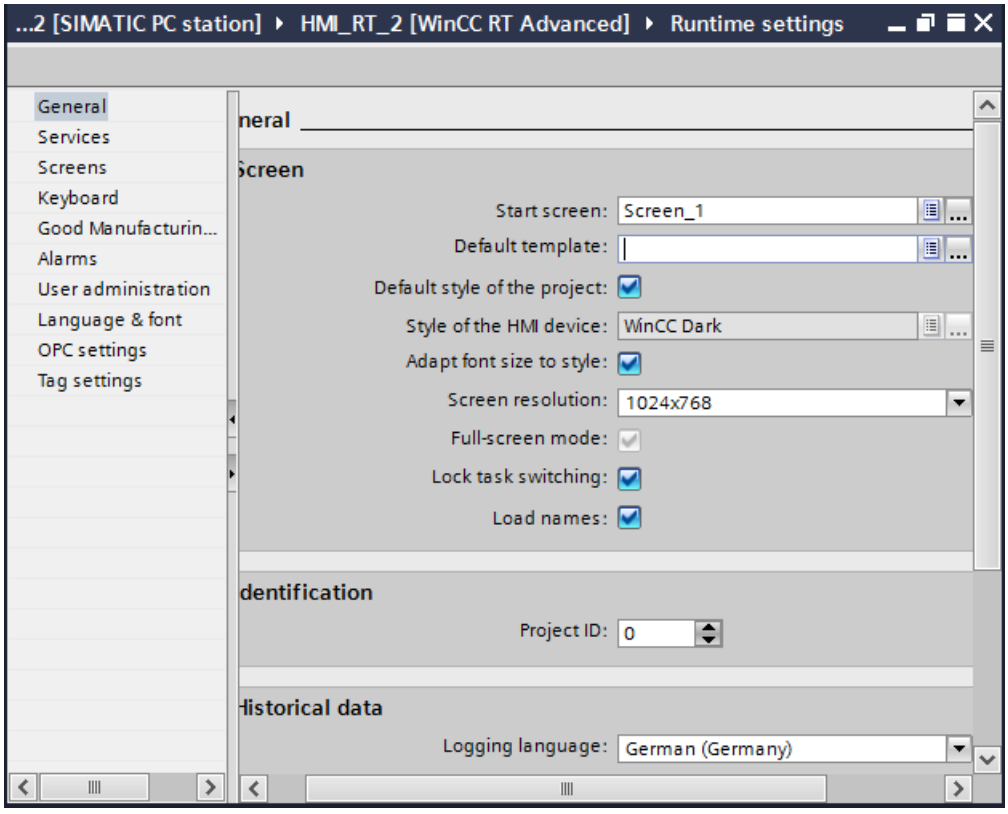


See also

- TIA Portal Information System > Visualizing Processes > Compiling and Downloading > Runtime Professional> Settings for Runtime > Configuring operator control in runtime > Configuring operator control in runtime (Professional)
- Locking of key combinations, Online Support under entry ID 44027453 (https://support.industry.siemens.com/cs/ww/en/view/44027453)

Configuration settings in WinCC RT Advanced

Access to the operating system during process operation is prevented if task switching is locked in the runtime settings under "General".



Note

Generally, for deactivating ongoing operation, a button can be provided on the user interface, which can only be actuated with the corresponding authorization and enables access to the operating system.

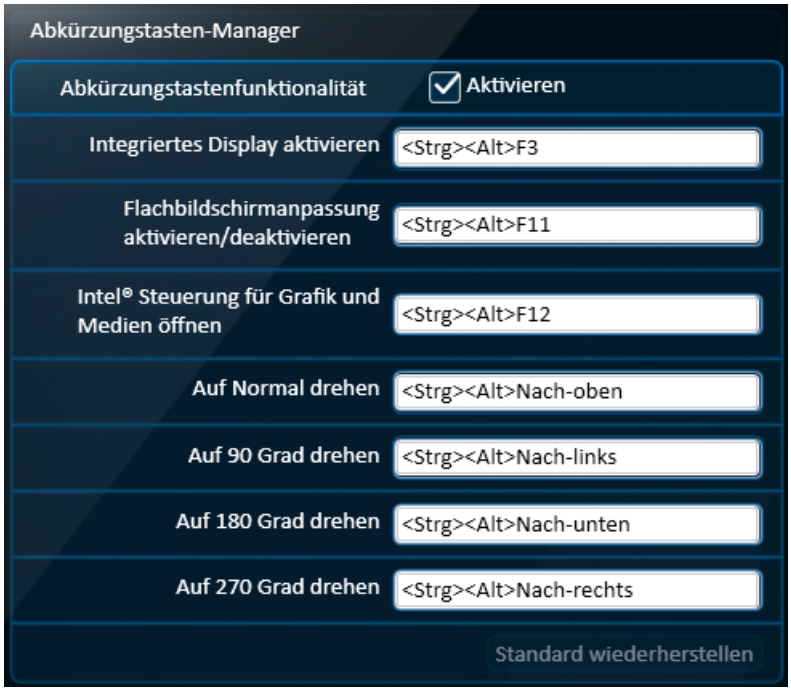
Preventing system access in object programming

It must be ensured 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 always in foreground" setting must be disabled in Windows.

Some graphics cards provide keyboard shortcuts for operation, which must be deactivated.



4.7 Data and information security

In the regulated environment, production processes and recorded data are controlled and securely stored in order to guarantee product quality verifiably. Secure handling of data is a basic requirement for compliant operation.

Relevant production data and operator inputs must be stored in accordance with national and international regulations for many years. Therefore, data and information security has many facets, some of which are explained here.

User administration

To ensure the protection of data, access must be regulated and limited to authorized users.

- WinCC project data, see chapter "Access control for TIA Portal project data (Page 58)"
- S7 program data, see chapter "Access protection for automation system (Page 58)"
- User administration for operator, refer to the chapter "Setting up the user administration for HMI devices (Page 48)"

Definition of a suitable infrastructure

- Planning of data storage as well as the input and output devices
- Secure storage of sensitive data with redundancy and access control

- Use of virus scanners, see chapter "Virus scanner (Page 42)"
- Defined startup characteristics and operation of the user interface, see chapter "Access control at the operating system level (Page 58)"

Organizational measures

- Planning and assigning the necessary access rights
- Supplemented with codes of behavior, such as handling of USB sticks
- Operating procedures for archiving, retrieval and possibly data migration

Adaptation of the operating system settings

During installation of the WinCC RT Advanced and WinCC RT Professional Runtime software, default settings in the Windows operating system are automatically adapted to the requirements of the software with SIMATIC Security Controller.

See also

- Chapter "Installation of the SIMATIC WinCC RT runtime software (Page 47)"

SIMATIC NET SCALANCE S

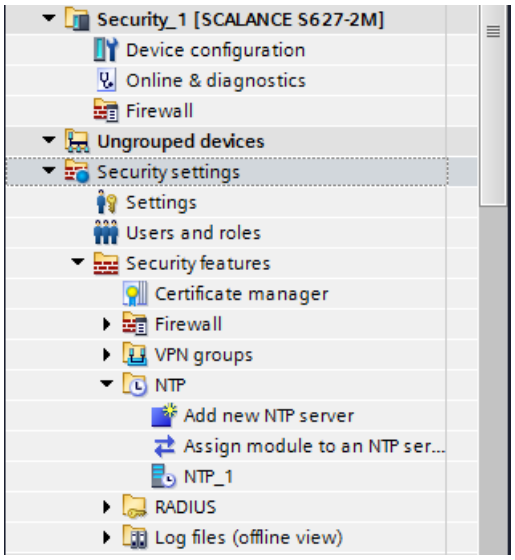
The SCALANCE S security modules form the core of the innovative safety concept of Siemens that protects networks and data. The protective function of SCALANCE S works in such a way that all traffic to and from the cell is controlled.

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

- Data espionage
- Data manipulation
- Unauthorized access

Security configuration in the TIA Portal

Security modules of type SCALANCE S or communication processors (CP) that are used to increase network security can be configured in the TIA Portal engineering system. These modules are integrated into the network in the Devices & networks editor. After the definition of a user who has authorization to configure the security settings, the editors for the security settings are displayed in the project tree.



In the NTP editor, NTP(secure) servers can be configured that safeguard the time synchronization in the network through additional encryption (see also chapter "Time synchronization (Page 81)").

See also

- TIA Portal Information System > Editing devices and networks > Configuring networks > Industrial Ethernet Security > Configuring security > General
- Manuals of the SCALANCE family
- "All-round protection with Industrial Security - Plant Security", Online Support under entry ID 50203404 (https://support.industry.siemens.com/cs/ww/en/view/50203404)
- "All-round protection with Industrial Security - Network security", Online Support under entry ID 92651441 (https://support.industry.siemens.com/cs/ww/en/view/92651441)
- "All-round protection with Industrial Security - System integrity", Online Support under entry ID 92605897 (https://support.industry.siemens.com/cs/ww/en/view/92605897)

Project Settings and Definitions 5

Projects are used to organize the storage of data and programs resulting from the creation of an automation solution. The data that makes up a project includes the following:

- Configuration data on the hardware structure and parameter assignment data for modules
- Configuration data for communication over networks
- Configuration data for the automation and HMI devices

The central data management ensures uniform consistency between automation and visualization. Once created, data is available in all editors, and changes or corrections are automatically updated throughout the project.

Both the process automation and the operator control and monitoring of the process can be implemented in a very flexible and customized manner. The automation program is prepared according to customer requirements. Standards developed for a specific customer can be used repeatedly in a carefully structured program.

A large part of the application software is configured for the HMI devices; additional functionality can be added with the aid of scripts.

5.1 Project setup

5.1.1 Creating a new project

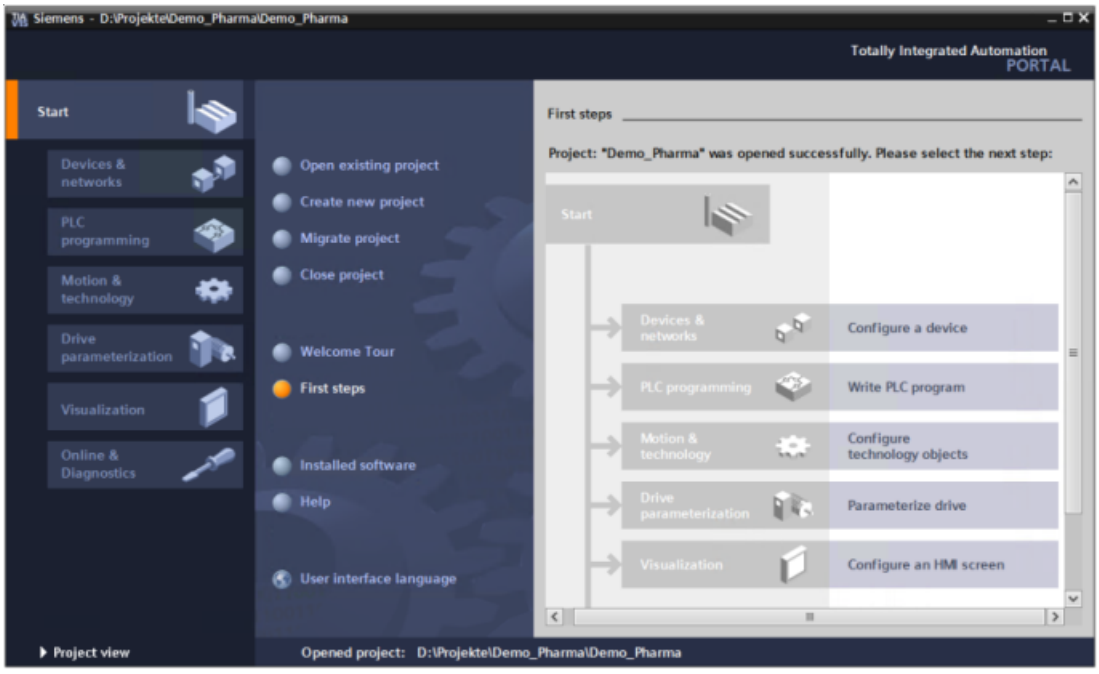
The TIA Portal is started for creating a new project. The TIA Portal offers two views, the portal view and the project view, which can be toggled.

- Select the "Create new project" entry in the portal view.
- Enter project name and path, or accept the suggested data.
- Click the "Create" button.

The remaining steps are listed in the TIA Portal.

- Configure a device
  Selection of the controller and HMI devices that are required for the automation solution. Network and connections can be configured.
- Write PLC program
  The programs are created for the individual controllers (PLCs).
- Configure an HMI screen
  The visualization is configured for the individual HMI devices.

A wizard provides support for performing each step and opens the project view at the suitable point.



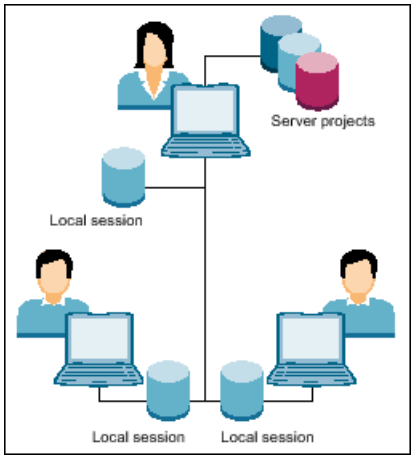
5.1.2 Multiuser Engineering

The Multiuser Engineering option allows multiple users to work together and simultaneously on Multiuser projects. Parallel processing offers significantly shorter configuration times, especially for extensive automation tasks. This requires a clear division of the work areas and thus the authority/responsibility within the TIA project. For example, this can be the separation between PLC programming and configuration of the user interface or the structuring of the automation task into individual technology areas for which the authorities are defined.

Method of operation

- Project management is located either on a local or external server.
- A connection based on https (certificate exchange) can be established between the different work stations.
- Multiuser Engineering has its own project management.
- Each user works independently in a local session, online or offline.
- Changes in the local sessions are transferred to the server project and checked in.
- Checked-in changes are displayed and can be applied by the other users.
- The users work either
  - across devices on the same objects
  - device-oriented on different objects
  - technology-oriented on different objects and devices

The following figure shows an example of a temporary multiuser server:



Multiuser server project

A standard project (single-user project) with all the basic settings such. For example, the hardware configuration (all devices, network connections), a basic structure for PLC programming, PLC tag tables, required languages and the like, will be converted to a multiuser server project. The person responsible for the TIA project assigns the tasks and responsibilities within the TIA project to the individual users.

Each user receives a secure connection to the multiuser server based on https (certificate prompt) and a local project session in which he works within his area of responsibility.

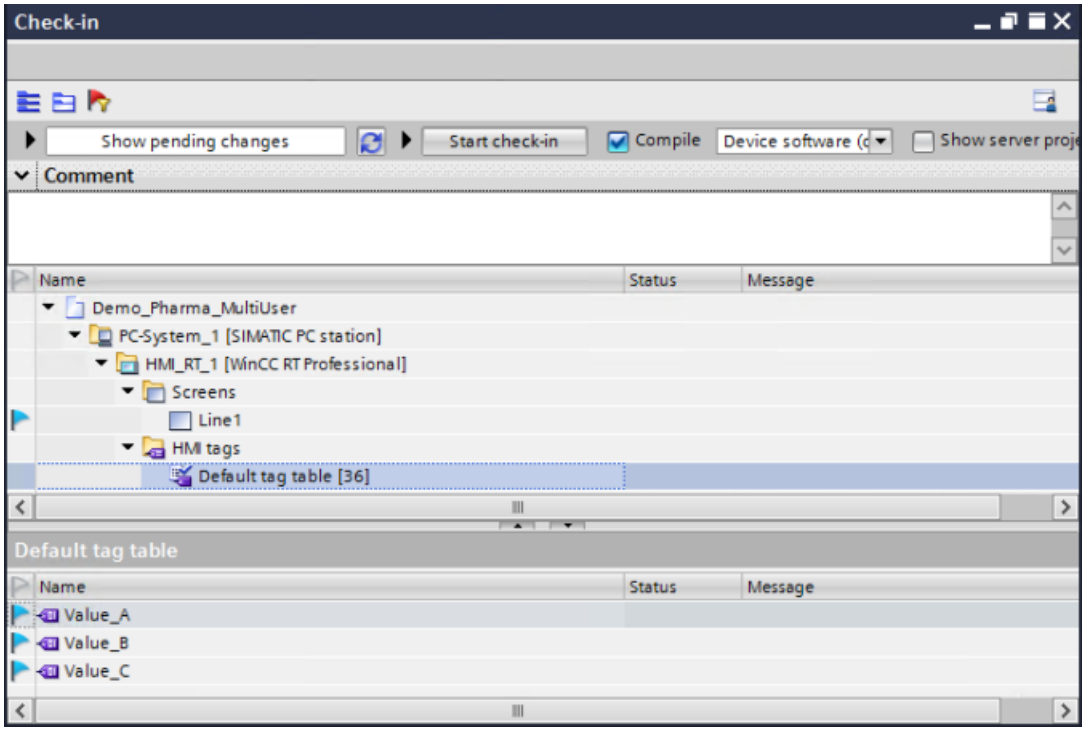
A special marking (gray flag) identifies the objects that can be edited in the context of multiuser engineering. All other configurations are performed centrally on the Multiuser server project.

If a user makes changes to an object in his local session, the color of the marking (blue flag) in front of the object in question changes in the project tree. Parallel to this, in every other local session, a marker (yellow flag) in front of the same object indicates that a user has made changes to this object.

The "Check in" and "Update" buttons are used to transfer the changes to the server project or to transfer the changes from other users to your own local session. The change status is marked in color in the selection.

Each user is responsible for checking in his changes as well as updating the local session.

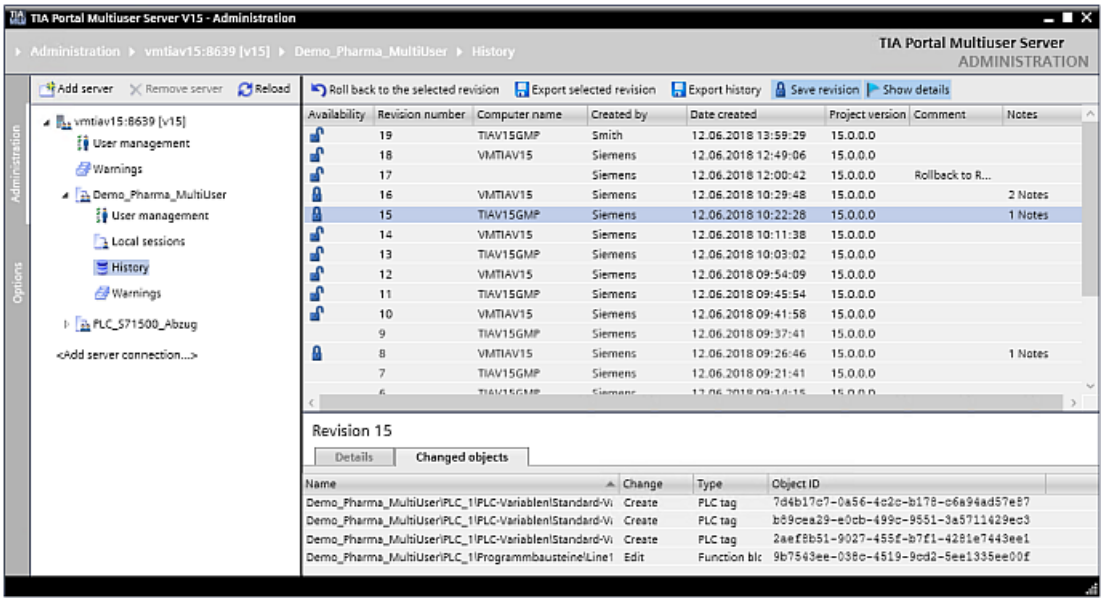
A local session can also be edited offline and checked in to the multiuser server project at a later time.



Management of a multiuser server project

The server project is assigned a revision number during check-in. A history lists the revision numbers with the time stamp of the creation, computer and user names. Details can be displayed for a selected revision number.

By default, the server project can be rolled back to one of the last 10 revision numbers. To store individual project revisions, these can be archived as needed, e.g. the delivery version of the server project. As a delivery version, the corresponding revision number is exported and converted into a single-user project. All administrative actions on the revisions have a comment function.

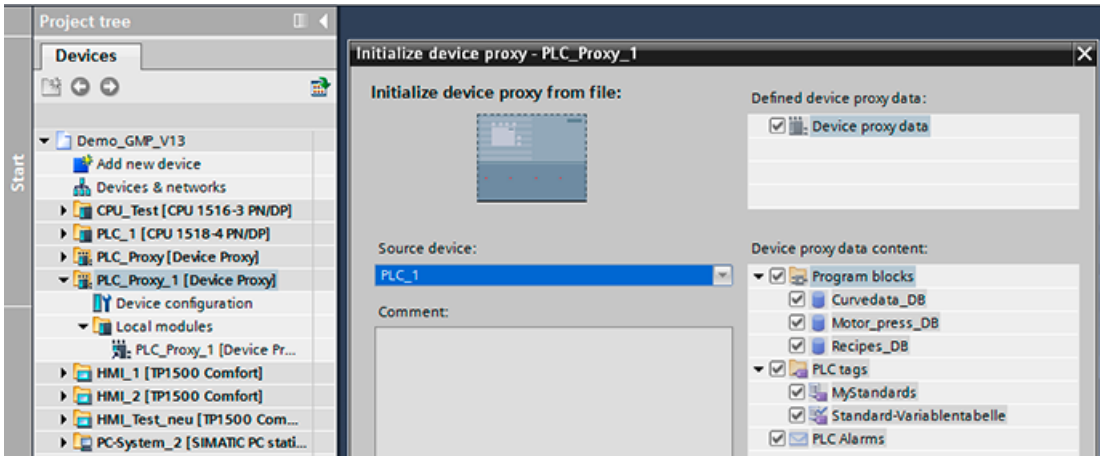


See also

- TIA Portal Information System > Using Team Engineering> Using Multiuser Engineering
- "Multiuser Engineering in the TIA Portal", Online Support under entry ID 109740141 (https://support.industry.siemens.com/cs/ww/en/view/109740141)

5.1.3 Inter Project Engineering (IPE)

Inter Project Engineering (IPE) is an alternative to multiuser engineering. A division is made here between the PLC programming and the visualization. The advantage of integration for tag connections and program messages is hereby retained. The PLC programming is performed in a TIA project. Definitions for tags and, if necessary, messages (for chronological messaging) that are required in the visualization are transferred to a device proxy file. In another TIA project for the visualization task, a PLC proxy device is added and initialized with the data from the generated device proxy file. In this way, the PLC tags are available in the customary manner. After changes to the PLC project, a device proxy file must be generated again and the associated PLC proxy device updated in the TIA project for visualization.



See also

- TIA Portal Information System > Using Team Engineering > Exchanging data with Inter Project Engineering (IPE)
- TIA Portal Information System > Visualize processes > Using global functions > Using controller data from other projects

5.1.4 Basic integrity check

Changes to essential project data (such as blocks, hardware configuration) made outside the engineering system or indicating defective data carriers are recognized by the "Basic integrity check" protection mechanism. If required, the check is activated in the Portal view before the TIA project is opened and, depending on the scope and application, can be time-consuming, especially in the multiuser engineering environment.

See also

- TIA Portal Information System > Introduction to the TIA Portal > User interface and operation> Starting, setting and closing the TIA Portal > Overview of the settings for the basic integrity check

5.1.5 Migration of existing projects

Projects from previous automation solutions can be migrated to the TIA Portal.

See also

- General procedure for migration in chapter "System Updates and Migration (Page 199)"
- TIA Portal Information System > Migrating projects and programs
- Migration of plants with SIMATIC (TIA Portal) – Visualization, Online Support under entry ID 76878921 (https://support.industry.siemens.com/cs/ww/en/view/76878921)

5.1.6 Integrated configuring with WinCC (TIA Portal) and SIMATIC Manager STEP 7

For technical or plant-specific reasons, it is sometimes necessary to continue creating the PLC program with SIMATIC Manager (> V5.4 SP3) and the visualization with WinCC (TIA Portal). Tag and alarm definitions in SIMATIC Manager are transferred using a file to a device proxy PLC directly into the TIA project for configuration of the visualization. Current HMI devices (e.g., Comfort Panels) can be integrated in SIMATIC Manager using a GSD/GSDML file in order, for example, to configure required connection parameters.

See also

- Combined configuration with WinCC (TIA Portal) and STEP 7 V5.x, Online Support under entry ID 73502293 (https://support.industry.siemens.com/cs/ww/en/view/73502293)

5.1.7 Working with multi-language projects

The TIA Portal supports the Unicode (UTF-16) format, which includes Asian languages. Multiple languages can be managed in parallel in a project and transfer to the HMI devices. The operator switches between the available languages for the operator interface using buttons.

It is possible to switch between languages for the following project texts:

- Alarm texts
- Labeling of screen objects, for example, buttons
- Display texts, texts relevant for operation
- Display names of recipes
- Text lists
- etc.

See also

- Chapter 13.14.5 in the "STEP 7 and WinCC Engineering" system manual, Online Support under entry ID 109755202 (https://support.industry.siemens.com/cs/ww/en/view/109755202)
- TIA Portal Information System > Visualize processes > Using global functions > Managing languages

5.1.8 HMI device wizard

A base structure for the visualization interface of an HMI device is created with the support of the HMI device wizard. When SIMATIC panels are added to a project, the wizard starts automatically; for HMI devices based on a PC system, the wizard can be started manually via the shortcut menu in the project tree.

The HMI device wizard guides you through a series of dialogs for creating the basic structure. The basic structure consists of a base screen with a toolbar, title bar, alarm line and various system screens for diagnostic purposes. Project-specific, empty plant screens can be added, so that these are already taken into account when selecting the screen. In addition, the screen background color, the screen resolution and the company-specific logo are defined.

See also

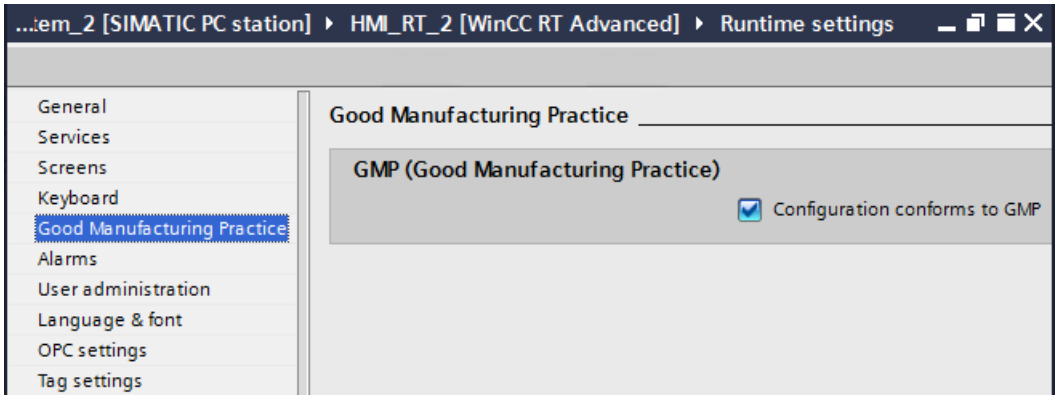
- TIA Portal Information System > Visualize processes > Using global functions > Working with the HMI device wizard > HMI device wizard basics (...)

5.1.9 GMP project setting in the Audit option

The WinCC (TIA Portal) Audit option for HMI devices of the Comfort Panel or Runtime Advanced type is provided specifically for GMP-relevant production plants. The option includes the following functions:

- Creating operator input alarms
- Creating an audit trail
- The "NotifyUserAction" system function
- Entering of electronic signatures
- Data archiving with checksum
- Identification of recipes as "GMP-relevant"
- Documenting the audit trail

The GMP setting is activated at the start of the configuration in the runtime settings editor. The above-listed functions are then offered and can be configured, see chapters "Creating operator input alarms (Page 97)", "Audit trail (Page 102)" and "Configuration for electronic signature (Page 105)".



5.2 Libraries

The engineering in the TIA Portal is supported by two libraries:

- Project library
- Global library

The project library is used to store programmed or configured software elements. In the PLC area, these are blocks and PLC data types developed specifically for the user or complete PLC devices. For HMI devices, user-defined WinCC objects, such as complete screens, tag tables, scripts, etc., all the way to complete configuration of HMI devices are stored. These user-defined blocks or objects are developed in detail, tested and qualified and are thus available as a project standard for multiple use in the project.

The global library is a cross-project library, the contents of which can also be used in other projects. By default, the global library contains master copies for buttons, control modules, and document templates for the project documentation. User-specific global libraries can be set up for centralized storage of user-defined objects and blocks, for example, from the project library.

The read-only export saves the content of a user-specific global library, e.g. for delivery to a customer. Changing a read-only library is no longer possible. The objects and blocks contained are inserted and interconnected in a project as usual by drag-and-drop. The objects themselves cannot be changed.

See also

- TIA Portal Information System > Using libraries > Library basics
- TIA Portal Information System > Using libraries > Library basics > Using global libraries > Creating a read-only global library
- Application example "Basic Process Library", Online Support under entry ID 109749508 (https://support.industry.siemens.com/cs/ww/en/view/109749508)

5.3 Object-oriented configuration for HMI devices

For the graphic design of the user interface, the toolbar offers a comprehensive set of objects and graphic elements.

Customized display and operating objects consisting of a configured group of objects are created as faceplates. The screen window technology is used for the display of a screen in the screen.

By storing configured objects, object groups and faceplates in libraries, they can be used repeatedly.

The objects stored there are available to all similar type HMI devices in the project ("Project Library") or in other projects ("Global Library").

For dynamization of faceplates and screen windows, it is preferable to use a user data type that bundles various tag types in a user-defined data structure for a process unit such as a motor. User data types are stored in the project library and are available throughout the project.

The object-oriented configuration is useful for:

- Configured objects and object groups
- Faceplates, see chapter "Faceplates (Page 76)"
- Screen windows, see chapter "Screen window (Page 77)"
- Pop-up screens, see chapter "Pop-up screen (Page 77)"
- User data types, see chapter "User data type (Page 77)"
- Project functions, see chapter "Project functions in the form of scripts (Page 78)"

Note

Configured objects or object groups, faceplates and user data types are created for the respective use case and tested with the customer before they are copied or instantiated in the configuration.

5.3.1 Master copies and types

The libraries mentioned in chapter "Libraries (Page 75)" each contain the two folders "Types" and "Master copies". Library objects can be created or used either as a master copy or as a type.

As a master copy, a configured object group is moved to the master copy area of the project library and can be used repeatedly in the project. Changes to the master copy are not transferred to the copies previously created. Master copies can also be stored in a global library for use in other projects.

Faceplates and user data types are created and maintained in the "Types" folder. These are based on the type-instance model. For example, when a faceplate is integrated in a process screen, a local instance of the type is created. Changes in the type are automatically transferred to all of its instances. If necessary, an instance of the type can be deleted.

A distinction is made between the Panel / RT Advanced and RT Professional device families when the faceplates are stored under Types. The faceplates can only be reused in the same type of device family.

See also

- TIA Portal Information System > Visualize processes > Using global functions > Working with libraries > Master copies and types

5.3.2 Faceplates

A faceplate consists of a grouping of objects which are tailored to the special requirements of the plant with respect to graphic representation and dynamization. The object properties and events used to dynamize the faceplate are individually defined in the faceplate editor. User data types are recommended for connecting the interface to the process screens.

A faceplate is always created as a type in the project library. A copy can be saved in the cross-project global library in the Types area. Thereafter, it is available in other projects as well.

There are significantly more options for designing and dynamization with WinCC RT Professional.

See also

- TIA Portal Information System > Visualize processes> Creating screens > Working with faceplates

5.3.3 Screen window

The "Screen window" control allows you to call a screen within a screen. This functionality is used, for example, to call a window for controlling a process unit (valve, drive). Such an operator control screen is configured once for a particular function and then opened as an instance in a screen window. The dynamization of a screen window is carried out based on user data types. When the screen is called, a tag prefix is transferred.

The screen window technology is only available in WinCC RT Professional.

See also

- TIA Portal Information System > Visualize processes > Creating screens > Display and Control Objects > Objects > Screen windows (RT Professional)

5.3.4 Pop-up screen

A pop-up screen is used to display additional information and, similar to the screen window, can be used to operate a process unit. A pop-up screen is displayed or hidden via a button. The dynamization is performed for each pop-up screen. Pop-up screens can be saved in the library as master copies.

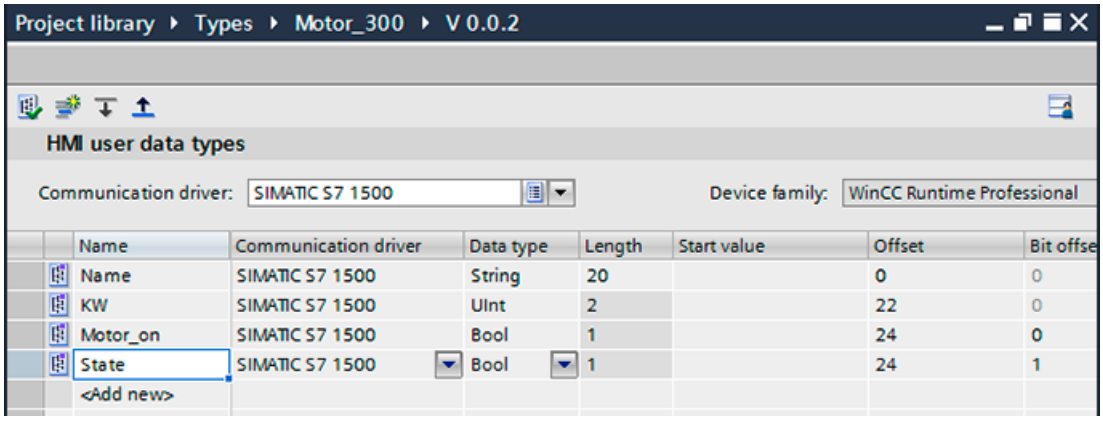
They are part of the functional scope for WinCC RT Advanced and Comfort Panels.

5.3.5 User data type

User data types are used for dynamization of faceplates and screen windows. For a process unit, such as a motor, a user data type is defined, which contains all tag types of the motor as elements.

Each user data type is created for a particular type of communication (SIMATIC S7-300/400, SIMATIC S7-1200, SIMATIC S7-1500, internal communication, etc.) and for a Panel / RT Advanced or RT Professional device family and can only be used in this environment.

The example shows a simplified form.



See also

- TIA Portal Information System > Visualize processes > Working with tags > Working with user data types (Panels, RT Advanced, RT Professional)

5.3.6 Project functions in the form of scripts

Customer-specific requirements that are not covered by the basic functionality can be realized in the form of functions or local scripts. A function consists of standardized system functions and/or user-defined functions.

If such user-defined functions are required repeatedly, they should be configured as project functions in the "Scripts" editor.

The function code is created one-time in the script, then tested and qualified. The function is then available for this HMI device and after moving it to the project library under "Master copy" it is also available project-wide for several HMI devices (see chapter "User-specific functions and scripts (Page 101)").

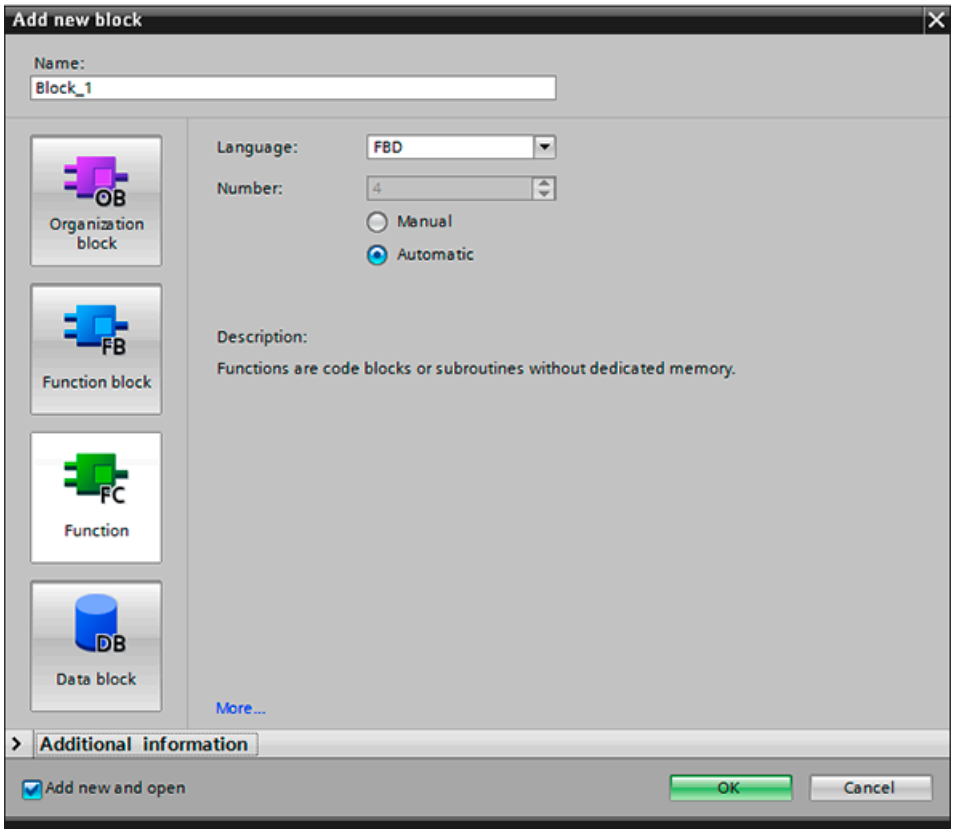
5.4 Block-based configuration of the automation software

The automation software is created using a modular approach. For information on the procedure for creating the user program, see chapter "Configuration for SIMATIC S7-1500 Automation Systems (Page 153)".

5.4.1 Blocks

The SIMATIC STEP 7 (TIA Portal) basic software provides different block types for structuring the software. The LAD, FBD, and STL programming languages and for certain blocks also the SCL programming language are offered for creating the software. Some CPUs also have the S7-GRAPH programming language for programming of step sequences.

- Organization blocks are called directly by the CPU either cyclically or acyclically. The call structure of the user program is started in these organization blocks.
- Function blocks communicate with an instance data block that stores the data of the interface.
- Functions are blocks whose interface data are not stored.
- Global data blocks are used for storage of program data.



Program code that is used multiple times in the user program is created once as a function or function block, then tested and qualified. For the call of a function block, only parameters have to be assigned. After the block is moved to the project library or a global library as a master copy or type, the block is available throughout the project and for other projects.

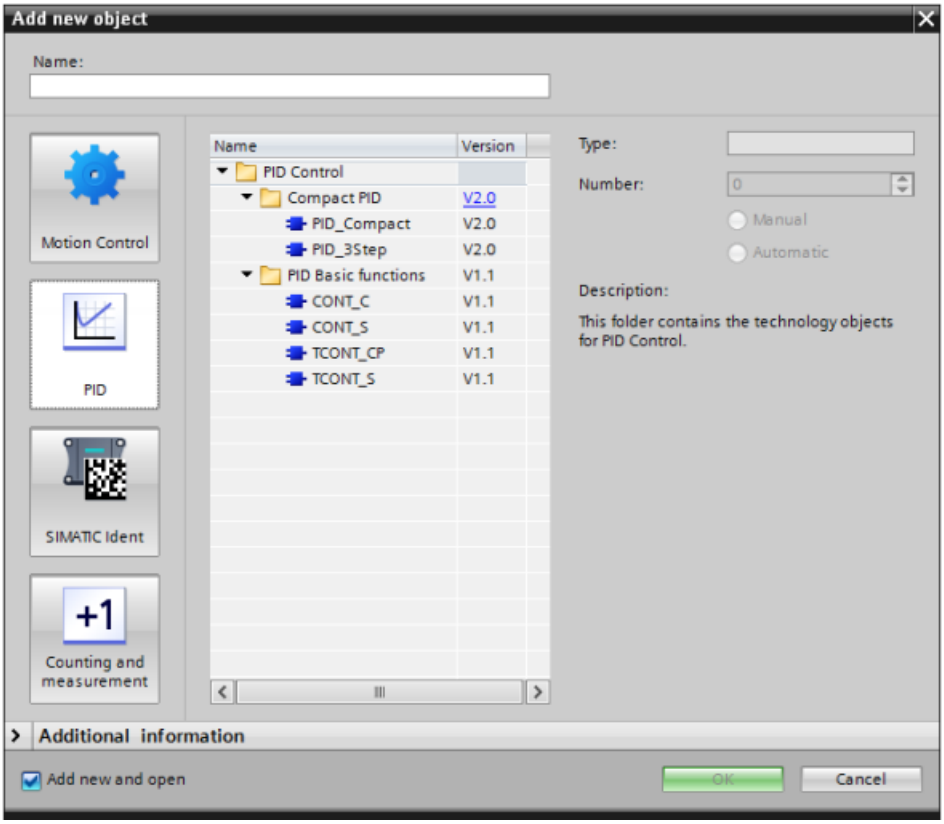
See also

- Chapter "Versioning examples in the area of the PLC (Page 93)"
- Chapter "Automation program (Page 153)"

5.4.2 Technology objects

Technology objects are standards for motion control, PID control and the rapid acquisition of a counter / measured value. The standard blocks are integrated in the automation software and parameters are easily assigned.

- Motion Control contains blocks for controlling stepper and servo motors with pulse interface.
- PID Control provides various closed-loop control blocks.
- SIMATIC Ident for easy parameterization of a SIMATIC Ident system
- Counting and measurement together with the high-speed counter provides for easy parameter assignment of counter modules.



5.4.3 PLC data types

A PLC data type (UDT) is a user-defined data structure that consists of multiple elements with different data types. For example, the interface data for a unit such as a motor or a recipe is mapped in a PLC data type. The PLC data type is used as a template for creating global data blocks and structured PLC tags. It is also used in the tag declaration of code blocks such as function blocks (FB) and functions (FC).

See also

- Chapter "Versioning examples in the area of the PLC (Page 93)"

5.5 Time synchronization

Time synchronization plays an important role in automated systems in the GMP environment. When interacting with automation (PLC) and/or HMI devices (WinCC RT Professional, RT Advanced, Comfort Panels), it is important that messages, alarms, trends and audit trail data are archived with synchronized time stamps.

In SIMATIC WinCC (TIA Portal), the time transmitted on the bus is by default the UTC (Universal Time Coordinated).

To ensure time consistency, all stations and controllers belonging to the automated system must be synchronized so that chronological processing (archiving of trends, messages) can be enabled system-wide. This applies to all computers in a Windows workgroup or within a domain.

Each time synchronization in the project is dependent on requirements. These are to be described in the functional specification.

The structure of the time synchronization must be carefully planned. One system component is selected as the timer for all other components. This time-based component acts as time master; all time-receiving components are time slaves. HMI devices with WinCC RT Professional can be integrated in a time synchronization via terminal bus or system bus (plant bus) or acquire the time from an NTP server. For panels or single-station systems with WinCC RT Advanced, either a time synchronization in the connection to the PLC or a "Set time of day" can be configured.

Time synchronization must also be activated for the TIA Portal Engineering station, otherwise problems could arise during the change loading.

Note

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

5.5.1 Concepts for WinCC RT Professional

The HMI device with WinCC RT Professional is integrated into either a workgroup or a domain.

Time synchronization in a Windows workgroup

The time synchronization in a workgroup should be realized via the WinCC server. In the Windows operating system, the computer can be configured as an NTP server that distributes the system time for the time synchronization in the network. A radio receiver, such as SICLOCK, can be used to feed the time in the network.

See also

- How to configure your PC as an NTP server, Online Support under entry ID 22144502 (https://support.industry.siemens.com/cs/ww/en/view/22144502)

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 synchronization of the domain server can also be realized using a time master such as SICLOCK.

Note

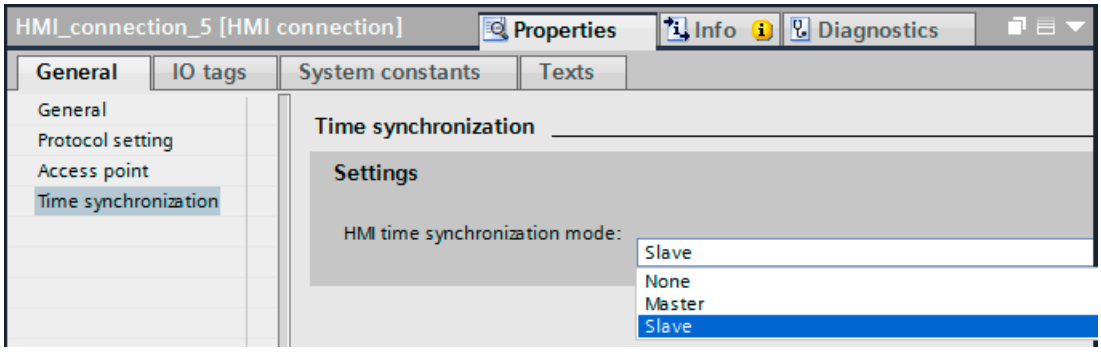
The time synchronization of the clients in the domain is realized using Microsoft system services.

See also

- Time synchronization - Time synchronization in the automation environment, Online Support under entry ID 86535497 (https://support.industry.siemens.com/cs/ww/de/view/86535497)
- Display format for the date, Online Support under entry ID 11377522 (https://support.industry.siemens.com/cs/ww/en/view/11377522)
- TIA Portal Information System > Editing devices and networks > Configuring devices and networks > Configuring networks > Industrial Ethernet Security > Configuring security > General > Configuring time synchronization
- TIA Portal Information System > Visualize processes > Communicating with PLCs > Communicating with SIMATIC S7 1500 > Configuring time synchronization (Basic Panels, Panels, RT Advanced)
- Chapter "Data and information security (Page 64)"

5.5.2 Concepts for HMI devices with WinCC RT Advanced

For a CPU and HMI devices of the RT Advanced or Comfort Panels type, time synchronization is activated in the direct or indirect connection between the devices. Here, the time can be specified by the HMI device (master) or by the controller (slave).



See also

- TIA Portal Information System > Editing devices and networks > Configuring devices and networks > Configuring networks > Industrial Ethernet Security > Configuring security > General > Configuring time synchronization
- TIA Portal Information System > Visualize processes > Communicating with PLCs > Communicating with SIMATIC S7 1500 > Configuring time synchronization (Basic Panels, Panels, RT Advanced)

Setting the time-of-day

As an alternative to time synchronization via the connection to the PLC, the time of day can be set in the CPU or in the HMI device. The "Set time-of-day" method does not have the same accuracy as the time synchronization, since frame and script runtimes are introduced. The device that serves as the time master must be defined within the system.

Note

If a network with an NTP server is available, the time synchronization should be realized preferentially using NTP mode.

See also

- Time synchronization between an HMI device and a SIMATIC PLC, Online Support under entry ID 69864408 (https://support.industry.siemens.com/cs/ww/en/view/69864408)
- Time synchronization - Time synchronization in the automation environment, Online Support under entry ID 86535497 (https://support.industry.siemens.com/cs/ww/de/view/86535497)
- Settings in Windows 7 in order to change the system time of the PC by means of WinCC RT Advanced, Online Support under entry ID 59203176 (https://support.industry.siemens.com/cs/ww/en/view/59203176)
- Chapter "Data and information security (Page 64)"

Daylight saving / standard time changeover

Daylight saving / standard time changeover is realized for panels using the "SetDaylightSavingTime" system function. This can be automated by a trigger of the PLC that evaluates the daylight saving / standard time changeover event.

See also

- TIA Portal Information System > Visualize processes > Working with system functions and Runtime scripting > Reference > Function list > System functions (Basic Panels, Panels, RT Advanced)

5.5.3 Concepts for the automation system

The time synchronization mode in the automation system determines the PROFIBUS and PROFINET connection types used.

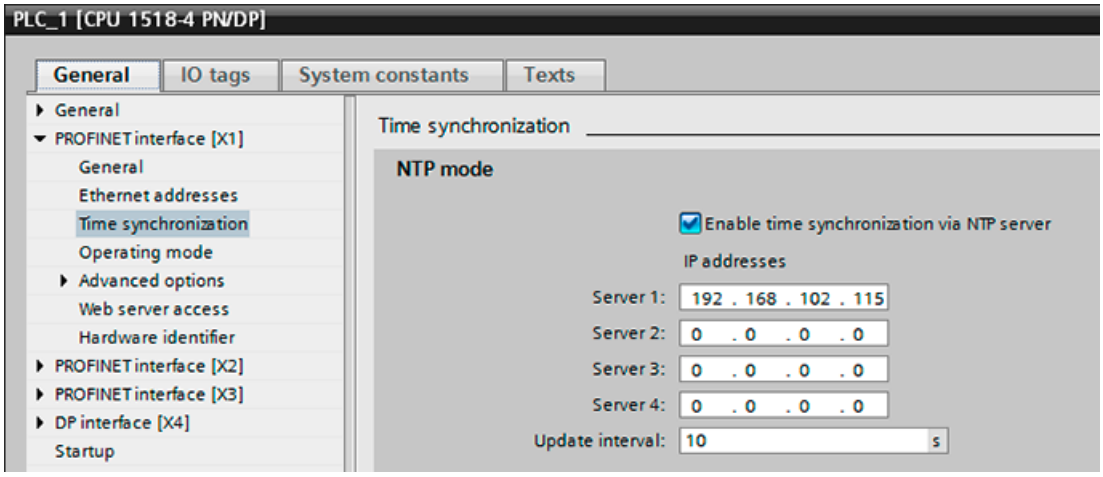
SIMATIC process

In the SIMATIC process, the time is set based on MMS time messages. In the group, the time messages come from either a SIMATIC time transmitter or a CPU, which acts as the time master. This process is offered for CPUs that are integrated in a PROFIBUS network (fieldbus system). The advantage of this method is the high accuracy.

NTP procedure

In the NTP process (Network Time Protocol) the device sends time-of-day requests to the configured NTP server at regular intervals. This is either the domain controller or one or more computers in the workgroup that are configured as an NTP server (for example, computer with WinCC RT Professional installation). The most exact time for the time synchronization is determined based on the answers. This method also works across subnet boundaries. It is used for CPUs with PROFINET interface.

Additional hardware such as CPs (communication processors) and SCALANCE switches control the network protocols, including for time synchronization, thus increasing the reliability in the network.



See also

- TIA Portal Information System > Editing devices and networks > Configuring devices and networks > Additional information on configurations > Functional description of S7-1500 CPUs (S7-1500) > Setting the operating behavior (…) > Time-of-day functions (…) > Time synchronization NTP mode (…)
- Chapter "Data and information security (Page 64)"
- Time synchronization (date and time) between WinCC Runtime Professional and an S7 controller, Online Support under entry ID 67518641 (https://support.industry.siemens.com/cs/ww/en/view/67518641)
- Time synchronization - Time synchronization in the automation environment, Online Support under entry ID 86535497 (https://support.industry.siemens.com/cs/ww/de/view/86535497)

GetClockStatus

The call of the GetClockStatus instruction in the PLC program reads out the status of the NTP time synchronization and indicates whether the automatic adjustment of the standard time and daylight-saving time is activated.

5.5.4 Time stamps of messages and process values

The specification (URS, FS) of a GMP-compliant plant must describe the way in which time stamping will be performed. The accuracy necessary for alarm and process value acquisition must be checked in detail. The following methods for time stamping the messages (bit messaging / program messages) can be used in parallel. The hardware for the automation and visualization must be selected accordingly.

Messages

Alarms from the CPU (AS) are displayed in the HMI device and logged. The alarm receives the time stamp either from the HMI device upon arrival of the alarm (discrete alarms) or from the CPU directly when it is created (controller alarms).

A discrete alarm is detected based on a bit change in the alarm tag. The HMI alarm system assigns the time stamp of the HMI device. The time stamp has a certain inaccuracy due to the acquisition cycle, bus delay time and time required for processing the alarm. Alarms present for a time shorter than the acquisition cycle are lost.

For monitoring the limits of tags in WinCC, an analog alarm is generated in the HMI alarm system if the defined limits are violated. The assignment of the time stamp is similar to that for discrete alarms.

The discrete alarm procedure and limit monitoring are easy-to-configure alarm procedures for panels, HMI devices with WinCC RT Advanced and single-station systems with WinCC RT Professional. In redundant systems or system configurations with multiple operator stations (WinCC RT Professional), program alarms are generated in the CPU for coordinated acknowledging and sending. These receive a precise time stamp directly when they occur in the CPU.

Standard blocks for generation of program alarms are offered that are tailored to the utilized CPU. For example, for the CPU S7-1500, the Program Alarm block; for the CPU S7-400, the Notify, Notify_8P, Alarm, Alarm_S/SQ, Alarm_D/DQ, and Alarm_8/8P blocks; for the CPU S7-300, the Alarm_S/SQ, Alarm_D/DQ, and Alarm_SC blocks in simple design.

Program alarms are transferred to the various HMI devices of the TIA project as controller messages. The assignment is made by an alarm class assignment.

Note

The time stamping of the program alarms in the CPU is more accurate than that of the discrete alarms and analog alarms that are only generated in the individual HMI devices. However, the configuration is much more complicated. In addition, the different CPU possibilities must be considered in the selection. Refer to the relevant CPU manuals and the block descriptions in the TIA Portal information system for restrictions relating to the system resources for simultaneously pending alarms.

See also

- TIA Portal Information System > Programming a PLC > References > References (S7-1200, S7-1500) > Extended instructions (...) > Alarms (S7-1500)
- TIA Portal Information System > PLC programming > References (S7-300, S7-400) > Extended instructions (...) > Messages (...)
- TIA Portal Information System > Visualize processes > Working with alarms > Basics > Alarm procedures > Overview of the alarm types (...)

Process values

By default, process values acquired and evaluated in the HMI device receive their time stamp at the time of their acquisition in the visualization system.

Archiving cycles are defined for cyclic archiving of the process values. The time stamp that is assigned when the process values are acquired contains the inaccuracy of the configured archiving cycle. Other archiving methods are "On change", "On demand" and cyclic selective triggered by an enable tag.

Archiving process values with a time stamp in the CPU can be configured with the AR_SEND block in the S7-400 automation systems. The AR_SEND block logs one or more process values in a data range that is transferred process-controlled to the archives of the WinCC Runtime Professional (TIA Portal) archiving system.

See also

- Process-driven archiving, Online Support under entry ID 23629327 (https://support.industry.siemens.com/cs/ww/en/view/23629327)
- TIA Portal Information System > Programming a PLC > Instructions > Instructions (S7-300, S7-400) > Extended instructions > Messages (S7-300, S7-400) > AR_SEND: Send archive data (S7-400)
- How do you configure process-controlled archiving for process tags with WinCC Runtime Professional, Online Support in entry ID 89292105 (https://support.industry.siemens.com/cs/ww/en/view/89292105)
- Archiving of process values and messages with WinCC (TIA Portal), Online Support in entry ID 109746939 (https://support.industry.siemens.com/cs/ww/en/view/109746939)

5.6 Configuration management

The configuration of a computer system consists of various hardware and software components, which can vary in complexity and range from commercially available **standard components** to specially customized **user components**. The current system configuration should be fully available at all times and easy to understand in a documented form. For this purpose, the system is divided into configuration elements, which are identifiable with a unique name and a version number and can be distinguished from the previous versions.

Definition of the configuration elements

In most cases, standard hardware components are used, for example PCs, controllers (PLCs), monitors, panels, etc. These are defined and documented by means of type, version number, etc. More work is required when customer-specific hardware is used, for more on this see chapter "Selection and specification of the hardware (Page 25)".

The software includes among the standard components, for example, the SIMATIC STEP 7 (TIA Portal) system software, SIMATIC WinCC (TIA Portal), the libraries included, further 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 they differ depending on various customer requirements and system characteristics.

Versioning of the configuration elements

Whereas the version ID of standard software cannot be influenced by the user / project engineer, the assignment of version numbers and a process for change control must be defined in work instructions for the configuration of the application software. Starting from the beginning of the application creation, all configuration elements should be maintained following a defined procedure for configuration management even if they are subject to formal change control only at a later stage.

Note

Chapter "Versioning of the application software (Page 87)" includes examples of how individual software elements can be versioned.

The procedure in case of changes in a plant already in operation should always be agreed with the process owner, see chapter "Operational change control (Page 195)".

See also

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

5.7 Versioning of the 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 after the FAT and to 2.0 after commissioning. All other changes are incremented in the minor version."

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

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

- Name
- Date

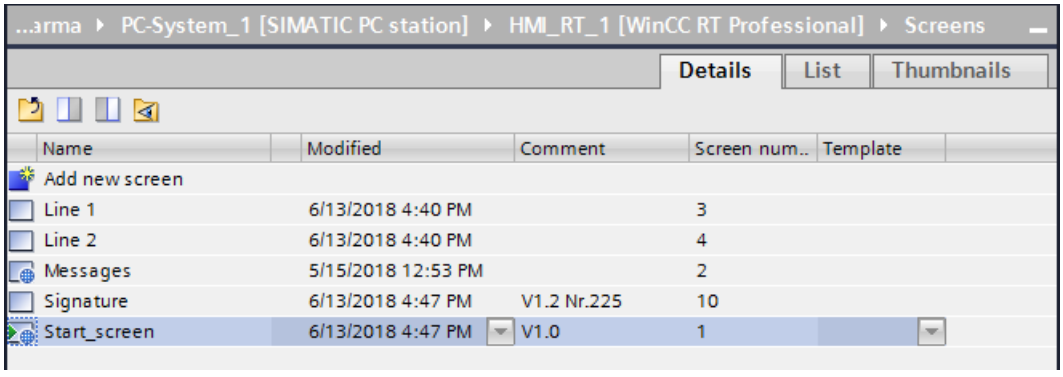
- Version number
- Comment on the change

The following chapters show various examples of software element versioning.

5.7.1 Versioning examples for the visualization level

Versioning of screens

The engineering system automatically records the creation date, the time stamp of the last change, and the Windows user logged on at the time. The data is retrieved if the "Screens" object in the project navigator is selected and the button is pressed in the toolbar on the project navigator.



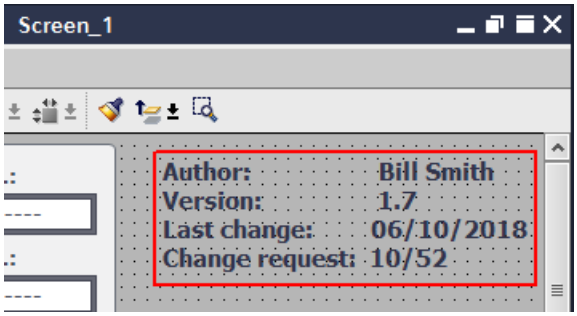
The Author and Creation date columns can be displayed using the column header.

See also

- TIA Portal Information System > Introduction to the TIA Portal > User interface and operation > Layout of the user interface > Overview window

Automatic versioning of the screens is not carried out; the version can be maintained manually in the file. Under Remark, for example, the last change can be manually maintained with the manually assigned version and a reference to the change number in the change request documentation.

Information for versioning, such as version ID, change date and name, can be stored in a static text field. In WinCC RT Professional it is practical to place the text fields for versioning in a separate screen level that can be shown or hidden as required. The display of the static text field during the process operation can generally be controlled by the "Display" object property or by the "Visibility" animation.



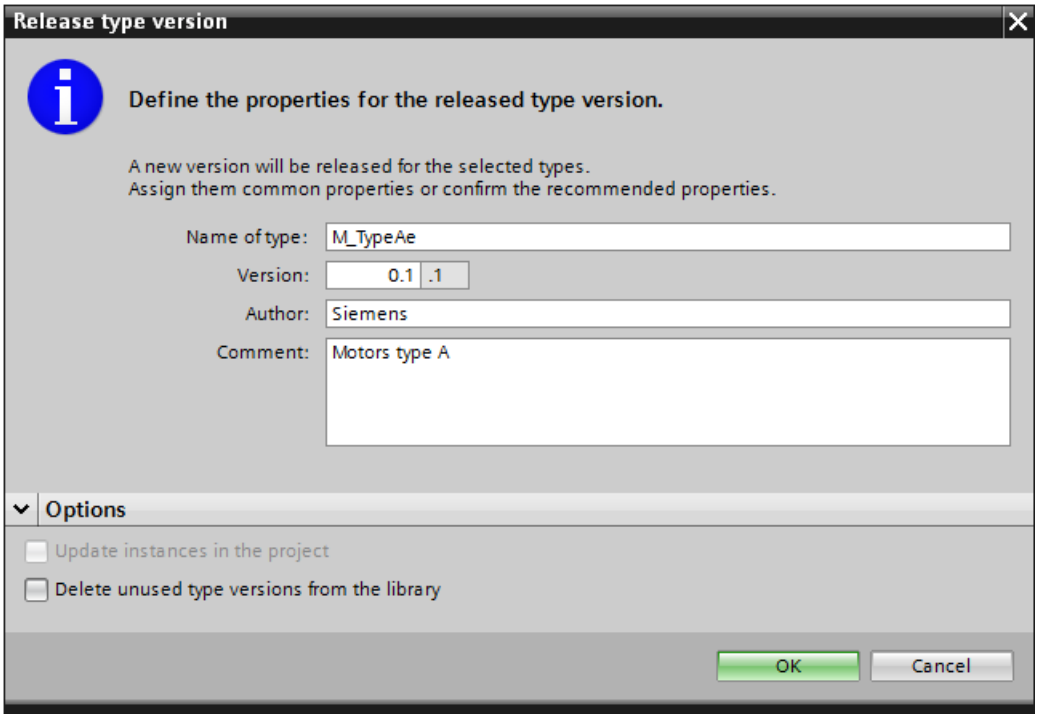
Note

Change details can be described, for example, in the relevant change request documentation.

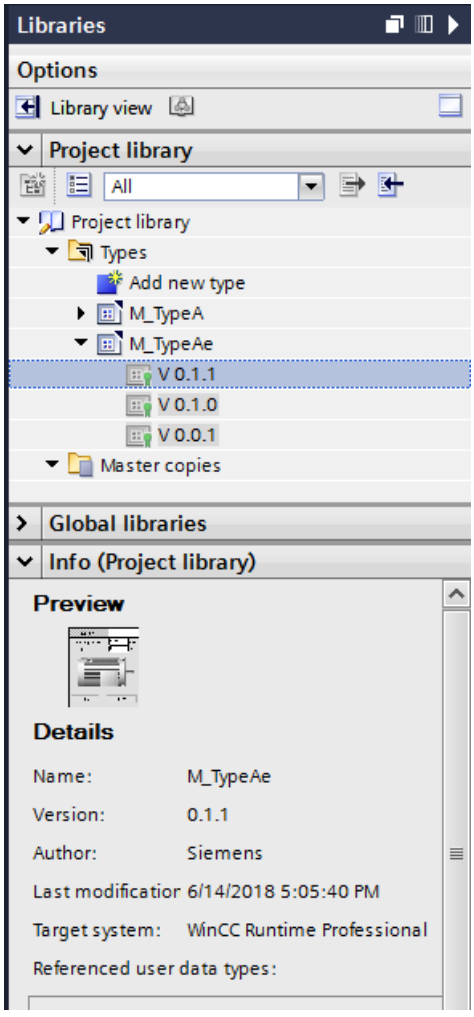
Versioning of faceplates

When the editing of a new faceplate is finished and it is released for use in the project data, the engineering system automatically sets the version 0.0.1. The first and second position of the version number can be specified on a user-specific basis. After the faceplate is edited and enabled again, the version number is incremented automatically in the third position. It is useful to enter a comment with information on the different versions. The current processing of a faceplate can be discarded by restoring the latest approved version.

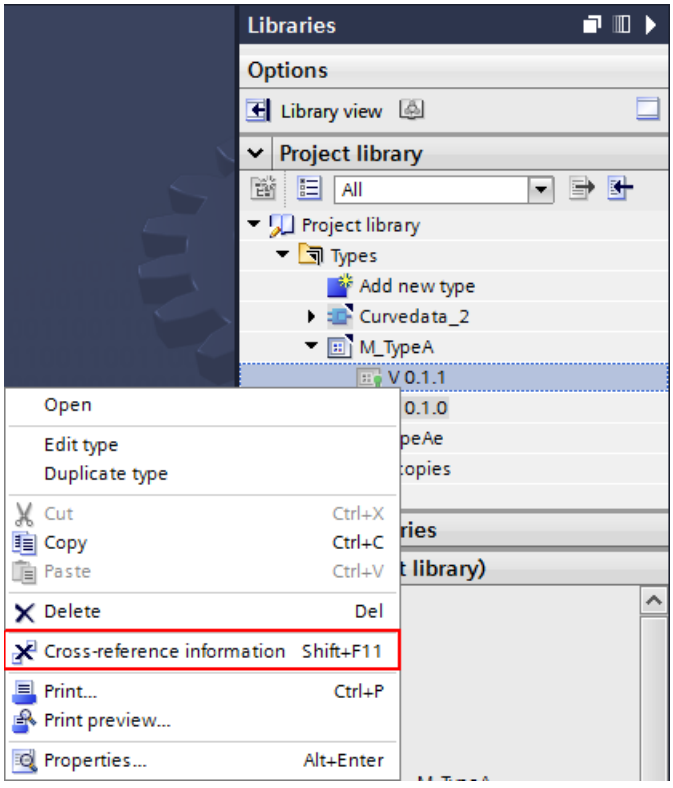
Changes in the faceplate are passed to all integrated instances only when the "Update instances in the project" property is activated at the time the faceplate is released.

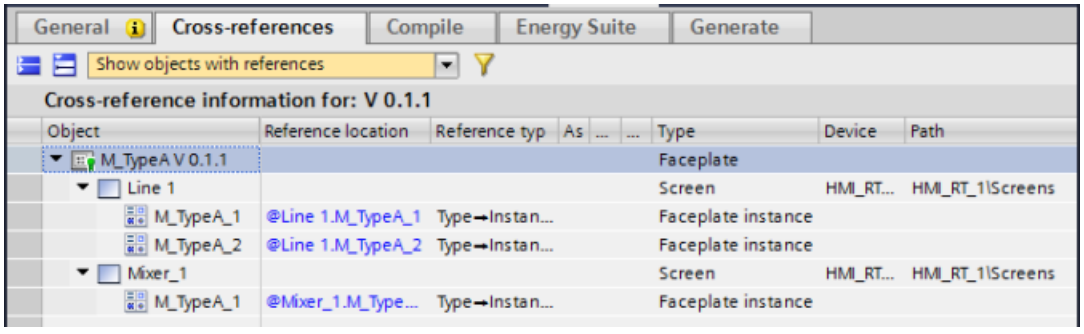


For additional information, see the properties in the information about the project library.



All versions are stored in the project library and can be deleted individually. Any version can be used in the project data. The use in the screens is listed in the cross reference for the version.





Versioning of VB / C scripts

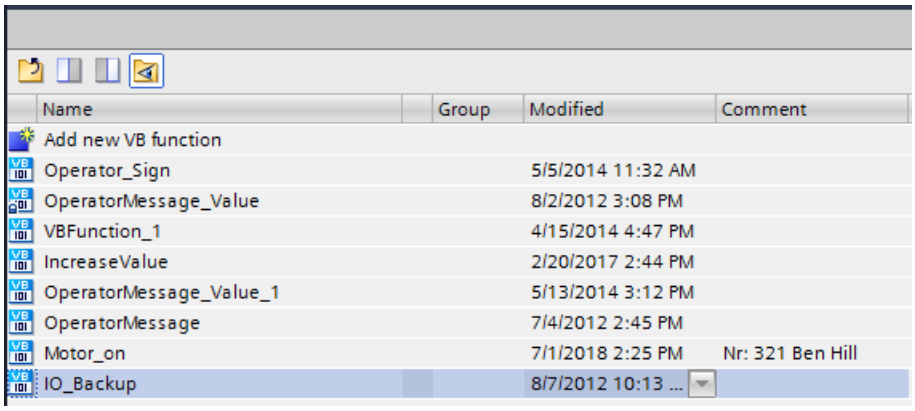
VB scripts or C scripts (only for WinCC RT Professional) are created in order to access tags and graphical screen objects during ongoing operation and to initiate screen-independent actions.

In addition, scripts are used to link functions that are initiated during process operation to individual properties of screen objects (e.g. in the case of operator input with the mouse).

Two different methods of script creation are distinguished in WinCC:

- Local scripts that are created directly for the property of an object in the "Screens" Editor. These scripts are part of the screen and are stored with the screen. Versioning is performed in the screen.
- Screen-independent scripts that are created in the "Scripts" editor and are available in function lists for repeated selection either with object properties or in the task scheduler.

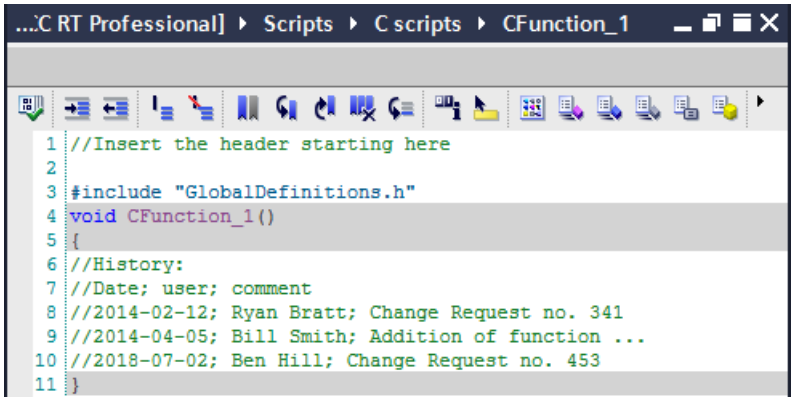
For VB / C scripts that are created with the "Scripts" editor, the engineering system records the last change date and the Windows user who is logged on at this time. To retrieve data, see the "Versioning of screens" area in this chapter.



Name	Group	Modified	Comment
Add new VB function			
Operator_Sign		5/5/2014 11:32 AM	
OperatorMessage_Value		8/2/2012 3:08 PM	
VBFunction_1		4/15/2014 4:47 PM	
IncreaseValue		2/20/2017 2:44 PM	
OperatorMessage_Value_1		5/13/2014 3:12 PM	
OperatorMessage		7/4/2012 2:45 PM	
Motor_on		7/1/2018 2:25 PM	Nr: 321 Ben Hill
IO_Backup		8/7/2012 10:13 ...	

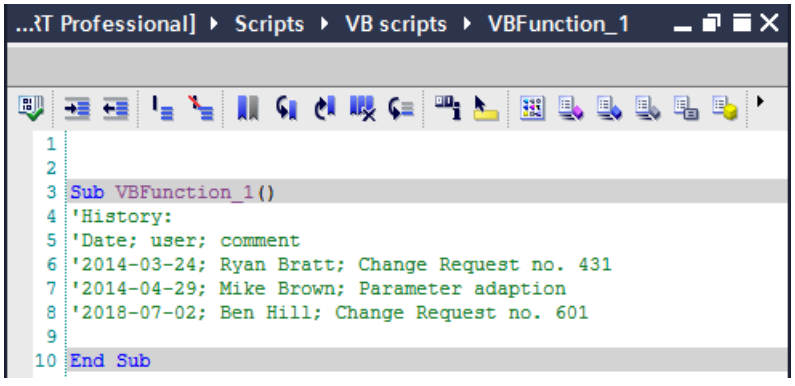
Note

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.




```
1  //Insert the header starting here
2
3  #include "GlobalDefinitions.h"
4  void CFunction_1()
5  {
6  //History:
7  //Date; user; comment
8  //2014-02-12; Ryan Bratt; Change Request no. 341
9  //2014-04-05; Bill Smith; Addition of function ...
10 //2018-07-02; Ben Hill; Change Request no. 453
11 }
```

Example for specification of the history in a C script

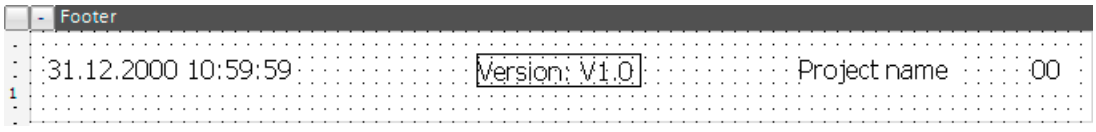



```
1
2
3  Sub VBFunction_1()
4  'History:
5  'Date; user; comment
6  '2014-03-24; Ryan Bratt; Change Request no. 431
7  '2014-04-29; Mike Brown; Parameter adaption
8  '2018-07-02; Ben Hill; Change Request no. 601
9
10 End Sub
```

Example for specification of the history in a VB script

Versioning of reports

The automatic issuing of a version ID in the report layouts is not supported. For manual versioning of different versions, a static field for entry of a version ID can be inserted in the report layout. The version ID must be kept up-to-date as specified in the SOP for configuration management. The following figure shows an example of a report layout footer with the additional entry field for the version.

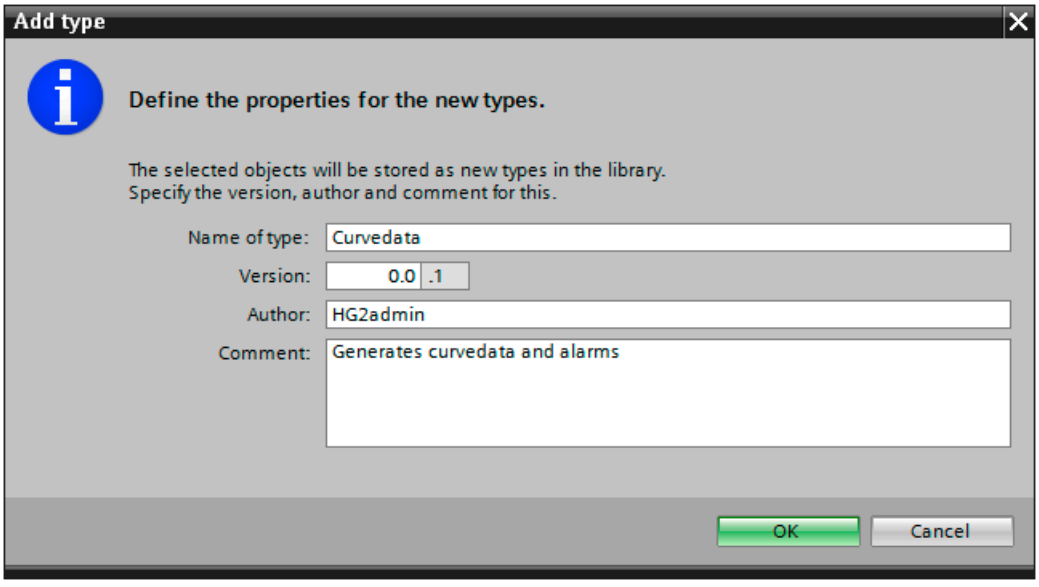


5.7.2 Versioning examples in the area of the PLC

Versioning of functions and function blocks

Functions (FC) and function blocks (FB) can be moved to the library as a master copy or a type. Storage as a type is only suitable if there are no absolute links to the PLC tag management or to data blocks. A warning message is output, if applicable.

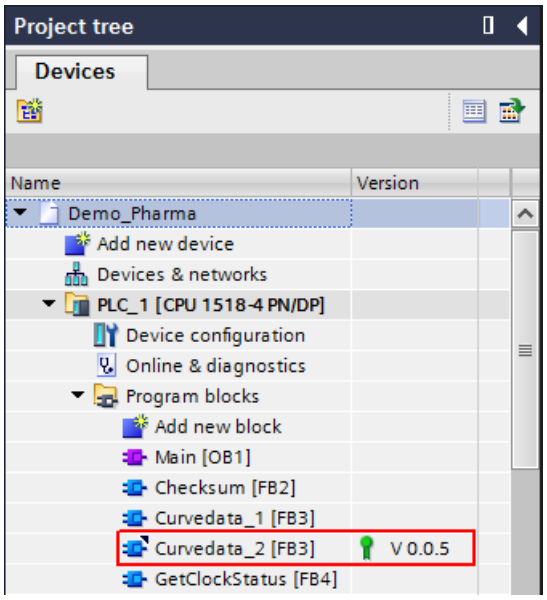
Upon first-time storage as a type, the name, author and content are entered and a version number is assigned. This is incremented automatically at the lowest position after a change and release. Depending on the extent of the change, the other two positions of the version number in the library can be manually adjusted.



The type/instance concept is activated when a block is moved to the library as a type. Instances of the block are used in the user program. The block can now only be edited in the library using the "Edit type" function. Editing in the block editor is blocked by write protection.

The master copy or type is moved from the library to the project tree for use in the user program. Block instances that are maintained as a type in the library are displayed with a specially

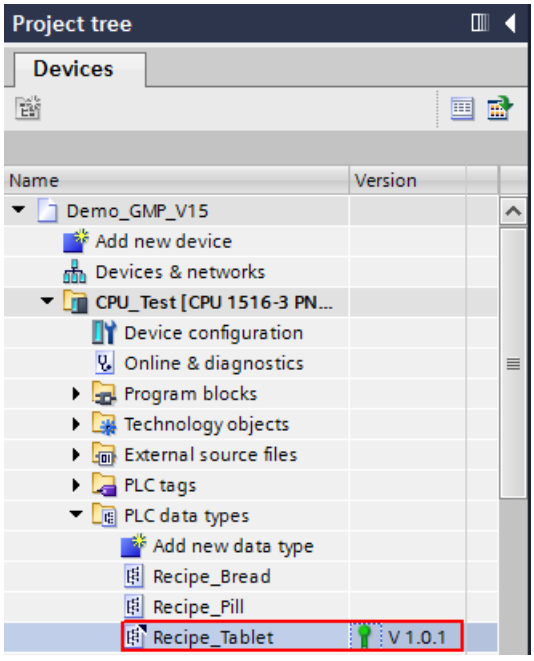
marked icon. If required, the version column for displaying the version number can be displayed in the project tree.



Versioning of PLC data types

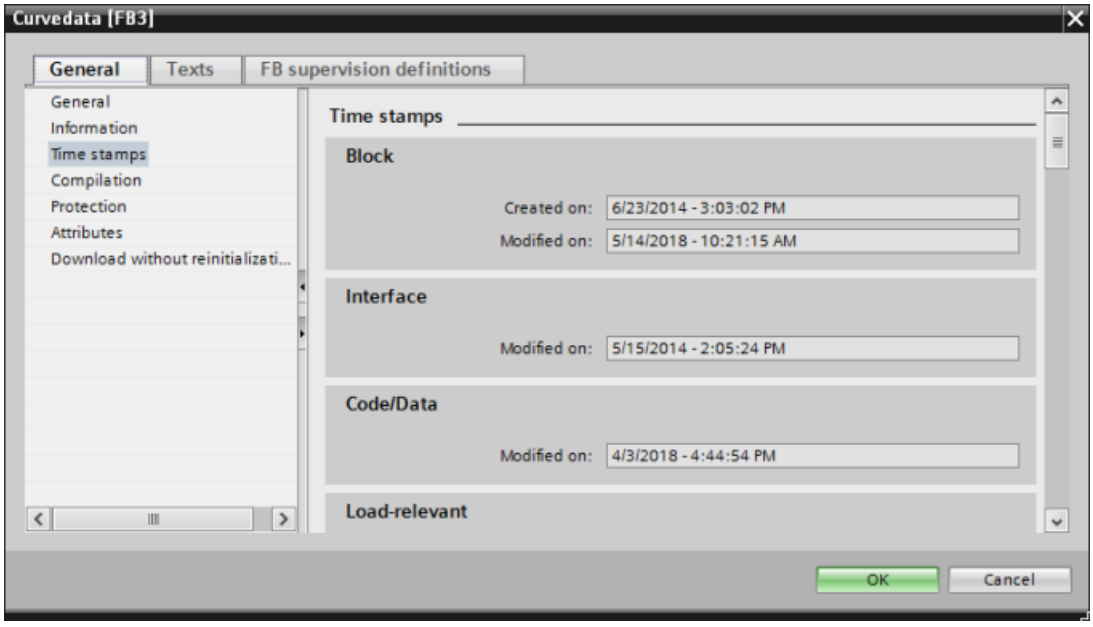
In the same way as functions and function blocks, PLC data types can also be stored as a master copy or type in the project library or in a global library. When a PLC data type is stored as a type, the type/instance concept is activated here as well. Name, author, comment and version number are specified. The PLC data type is then further maintained in the library.

PLC data types that are used as an instance in the program can be recognized in the project tree based on the marked icon. The version number is displayed in the version column, which can be displayed if necessary.



Time stamping within the PLC

The TIA Portal engineering system performs an exact time stamping for all blocks. This serves as the basis for the consistency check for the compilation and for downloading of changes to the CPU.



See also

- TIA Portal Information System > Programming a PLC > Creating and managing blocks > Specifying block properties > Block time stamps

5.8 Project management with Teamcenter

Teamcenter is a Product Lifecycle Management (PLM) platform that handles the central management of machine information. The "TIA Portal Teamcenter Gateway" option is used to connect the TIA Portal to a Teamcenter server. TIA Portal projects and global libraries are centrally managed there.

The TIA Portal project or the global library is saved to the Teamcenter server from the TIA Portal Engineering interface or saved as a new revision or as a new element. A new ID is hereby assigned either automatically or manually.

The "Check out" and "Check in" functions ensure that only one user has access to the project data. A separate user administration ensures controlled access to the Teamcenter.

The filing in the Teamcenter provides an overview of the history of TIA projects and global libraries.

Note

Work sequences between TIA Portal Gateway and TIA Portal Multiuser Engineering are not supported.

See also

- TIA Portal Information System > Editing projects > TIA Portal Teamcenter Gateway
- Digitalization with TIA Portal: PLM integration of automation technology, Online Support in entry ID 109749107 (https://support.industry.siemens.com/cs/ww/en/view/109749107)

5.9 TIA Portal Cloud Connector

The "TIA Portal Cloud Connector" option is used for the online connection between a virtual environment (private cloud) in which the TIA Portal is operated via Remote Desktop and the local PC interface of a device connected to the SIMATIC hardware (PLC) is.

Note

Use of the TIA Portal Cloud Connector is only intended for engineering work in the TIA Portal.

See also

- TIA Portal Information System > Using online and diagnostics functions > Connecting devices online> View in online mode
- Boundary condition for using the TIA Portal Cloud Connector, Online Support in entry ID 109739390 (https://support.industry.siemens.com/cs/ww/en/view/109739390)

Configuration for WinCC RT Professional 6

In a complete automation solution, SIMATIC WinCC (TIA Portal) takes over the operator control, monitoring and data archiving functions. The connection to the automation level is by means of high-performance process interfacing.

This chapter explains instructions and recommendations for the configuration of WinCC RT Professional in the GMP-mandatory environment. The configuration of HMI panels and WinCC RT Advanced is covered in chapter "Configuration for WinCC Comfort / WinCC RT Advanced (Page 127)".

See also

- "STEP 7 and WinCC Engineering" system manual, Online Support under entry ID 109755202 (https://support.industry.siemens.com/cs/ww/en/view/109755202)

6.1 Creating the graphic user interface

To visualize the plant or process, process screens for operator control and monitoring are created according the specified requirements. Available elements are described in chapter "Object-oriented configuration for HMI devices (Page 75)".

The HMI device wizard can be used to configure a basic structure for the visual interface and the screen resolution. For complex processes involving several process screens, we recommend defining a system for screen selection and screen navigation. SIMATIC WinCC provides the editor menu bars and toolbars for implementation.

Both the overview graphics and the operator input 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.

A large number of ready-made graphical objects in the formats EMF, WMF and SVG are available (independent of a library) for the creation of screens directly in the Engineering System under Tools > Graphics. The graphical objects are sorted according to machine and plant components, measuring devices, operator controls and buildings and can simply be added to a screen by drag-and-drop and adopted as required.

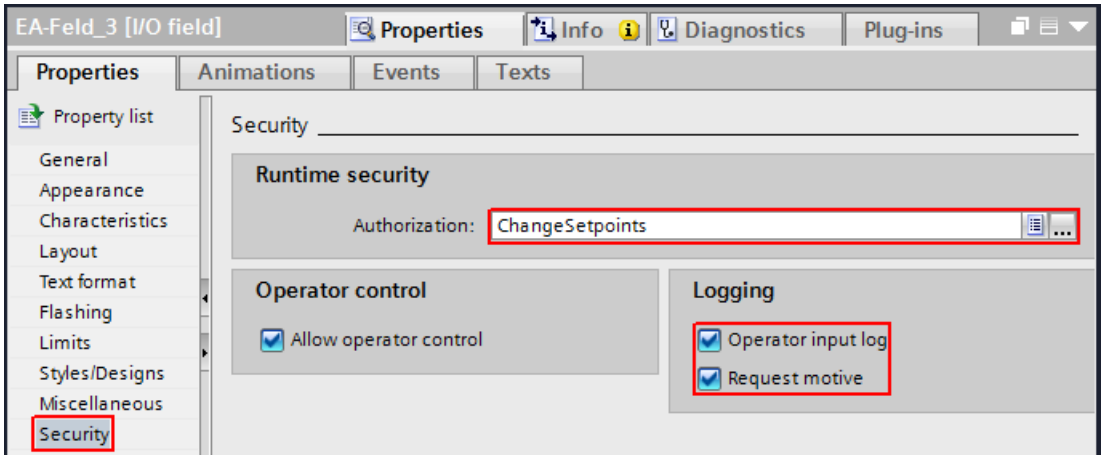
6.2 Creating operator input alarms

For plants that are operated in the GMP environment, the international regulations, such as US 21 CFR Part 11 and EU GMP Guide Annex 11, require traceability of operator inputs that influence GMP-relevant data.

GMP-relevant operator inputs made using input / output fields or buttons must therefore be configured such that an operator input alarm is generated. This operator input alarm is recorded in the alarm logging with time stamp, user ID, old value and new value.

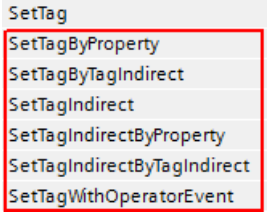
Input / output field

The generating of an operator input alarm when a value changes in an I/O field object is set in the "Security" object property. A system-side operator input alarm is generated when the "Operator input log" property is selected in the "Archiving" area. If the "Request motive" property is selected, the system opens a window for entering a comment after the value is applied. The corresponding operator input right is configured in the "Authorization" property under "Security in Runtime".



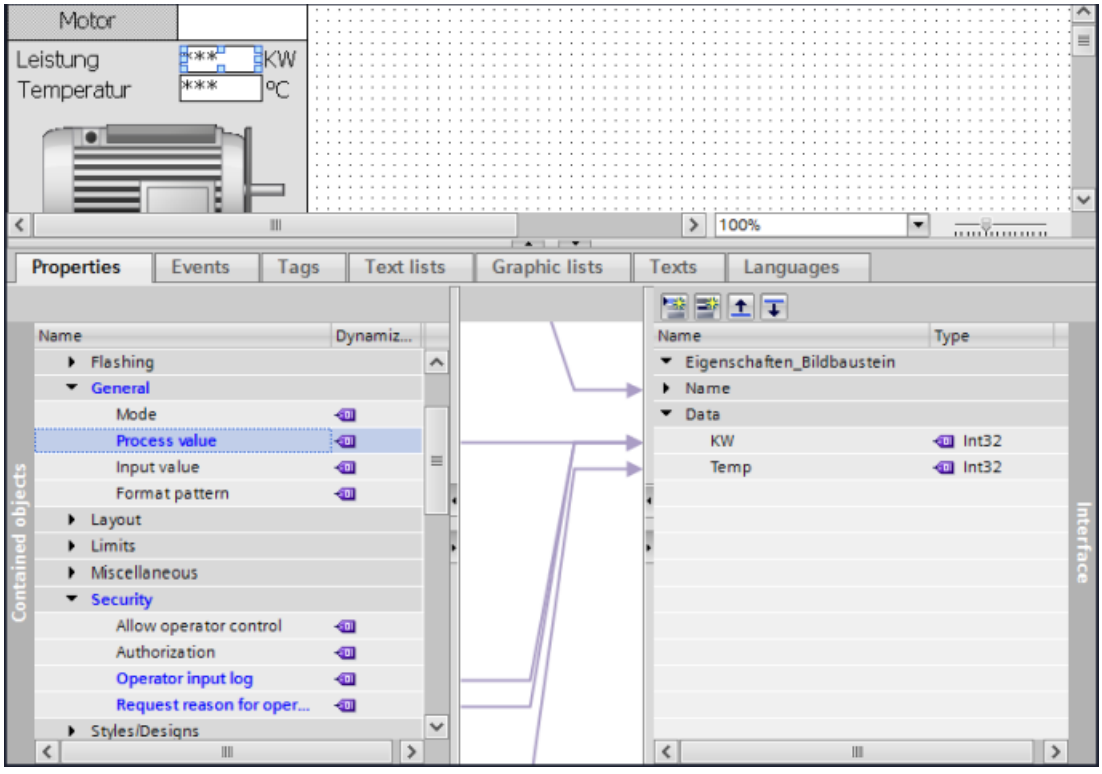
Button

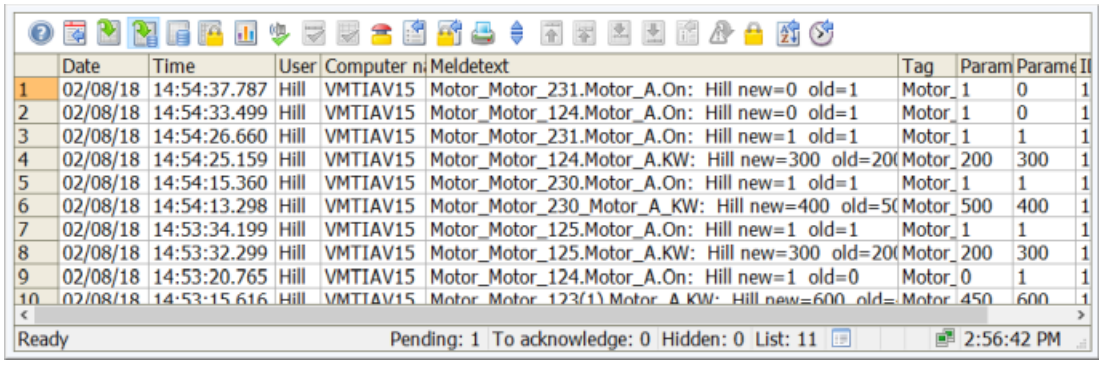
For the changing of tag values via a button, a system function is attached to an event of the button. A set of system functions that also create an operator input alarm is available for this. However, the entry of a comment/motive cannot be activated.



Operator input alarms in combination with faceplate types

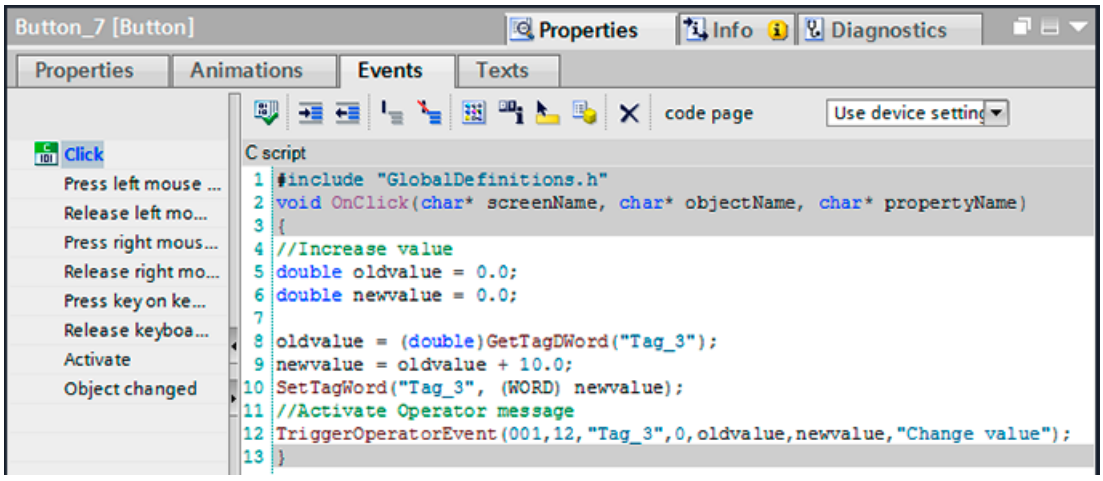
Operator input alarms can also be generated if the I/O field is integrated in a faceplate. For this purpose, the property "Operator input log" is activated for the object property "Security" in the faceplate on the I/O field and, if necessary, the property "Request reason for operation". The process value of the I/O field is placed on the interface of the faceplate. When a faceplate instance is inserted in a process screen, this interface is connected to the corresponding tags. If the value in the faceplate is changed, an operator input alarm is generated by the system, in which the tag name with the old value and new value for this faceplate instance is documented. The authorization for operation of the faceplate is specified for each integrated instance.





Script functions for value changes

Alarms for documenting operator interventions can also be configured in addition to the system-generated operator input alarms. The TriggerOperatorEvent system function is provided for integration in a C script. Alternatively, a VB script can be created by calling a pre-configured user alarm and supplying it with the appropriate process data. The scripts are attached to an object event in a process screen.

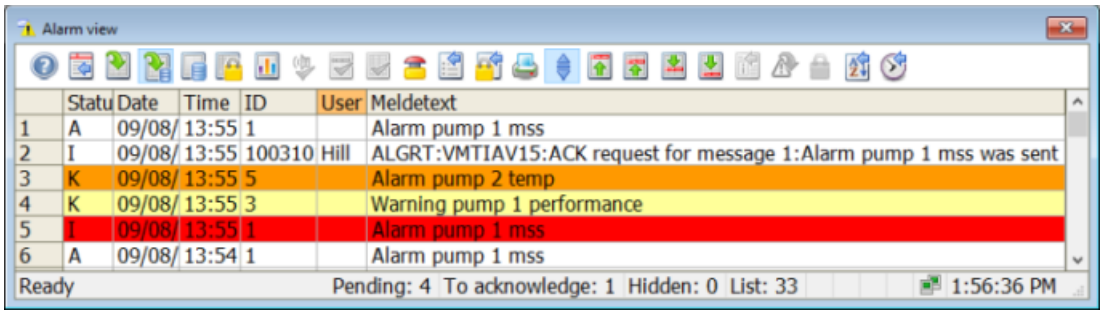


See also

- TIA Portal Information System > Visualize processes > Working with messages > Working with messages > Configuring messages > Configuring messages (RT Professional) > Configuring user messages (...)
- TIA Portal Information System > Visualize processes > Working with system functions and Runtime scripting > Reference > C scripting (RT Professional) > System functions (...) > TriggerOperatorEvent (...)
- Chapter "Configuration for electronic signature (Page 105)"

Acknowledgement of alarms as operator input alarm

Various operator actions (locking, releasing, hiding, showing, acknowledging) in the alarm view can be documented with an operator input alarm. For example, for the acknowledgment of an alarm, a system alarm is generated containing the time stamp of the acknowledgment, the logged-on user and a reference to the acknowledged alarm.



6.3 User-specific functions and scripts

Customer-specific requirements are implemented using system functions and/or user-defined functions.

System functions are system-tested standard functions that are already integrated in the TIA Portal.

User-defined functions or local scripts based on VB script or C script are user-written programs that are categorized as software category 5. This type of software is developed in order to meet customer-specific requirements not covered by the standard functions. In this case, a greater validation effort must be calculated in the form of detailed functional and interface descriptions and documented tests, see chapter "Software categorization according to GAMP Guide (Page 185)".

System functions are processed parallel to user-defined functions in a "function list" or integrated in user-defined functions or "local scripts". A "function list" is defined for an object event, and "local scripts" are attached directly to an object property. The task scheduler provides additional options for executing scripts.

See also

- VBS information and VBS programming tools in WinCC (TIA Portal), Online Support under entry ID 59885894 (https://support.industry.siemens.com/cs/ww/en/view/59885894)

Note

For creation of user-specific functions and scripts, the programming guidelines should be defined in project- or department-specific instructions (SOP coding standards, naming conventions, style guide, etc.).

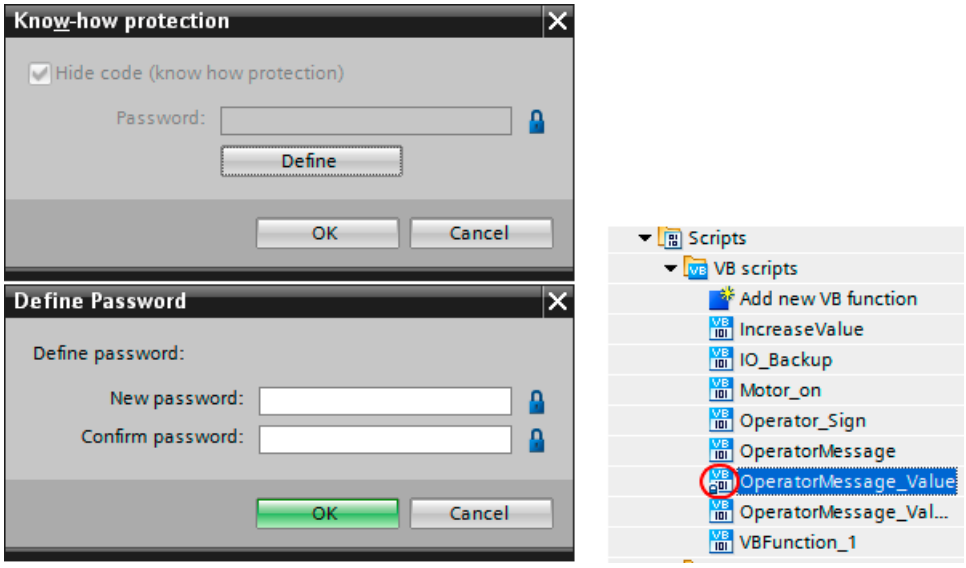
Know-how protection of user-defined functions

User-defined functions such as VB script or C script can be password protected. A password is required to open and edit the function. The protection is maintained, even if the protected function is moved to the library. Password protection can be canceled if the password is known.

Protected functions are identified in the project tree by a lock in the icon.

See also

- TIA Portal Information System > Visualize processes > Working with system functions and Runtime scripting > Safeguarding from customized functions
- "STEP 7 and WinCC Engineering" system manual, chapter 13.9.6 "Protecting user-defined functions", Online Support in entry ID 109755202 (https://support.industry.siemens.com/cs/ww/en/view/109755202)



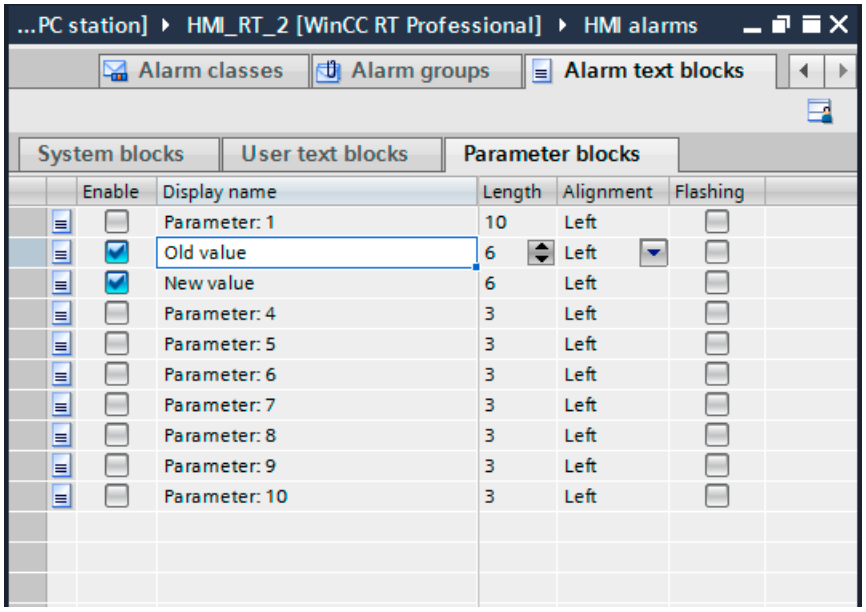
6.4 Audit trail

The recording of an audit trail for user actions with GMP-relevant data is implemented in the alarm system in WinCC Professional.

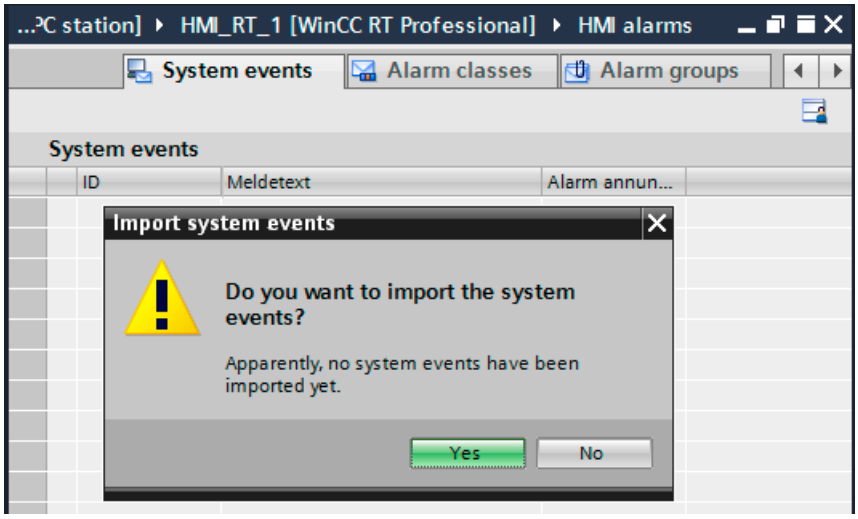
Operator inputs using input/output fields or buttons can be configured in the "Screens" editor such that an operator input alarm is generated by the system. (for configuration, see chapter "Creating operator input alarms (Page 97)")

Note

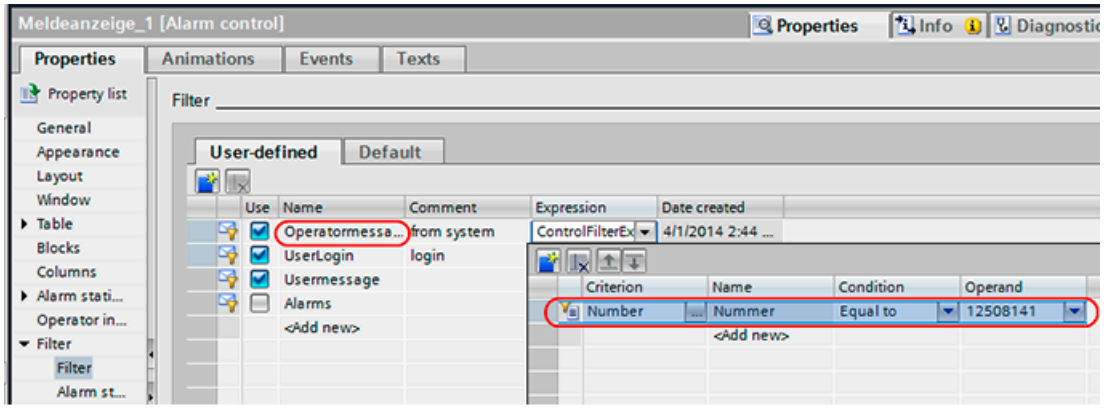
The generated operator input alarm is a system alarm for which WinCC automatically enters the old value in parameter block 2 and the new value of parameter block 3. Therefore, we recommend renaming parameter blocks 2 and 3 accordingly.

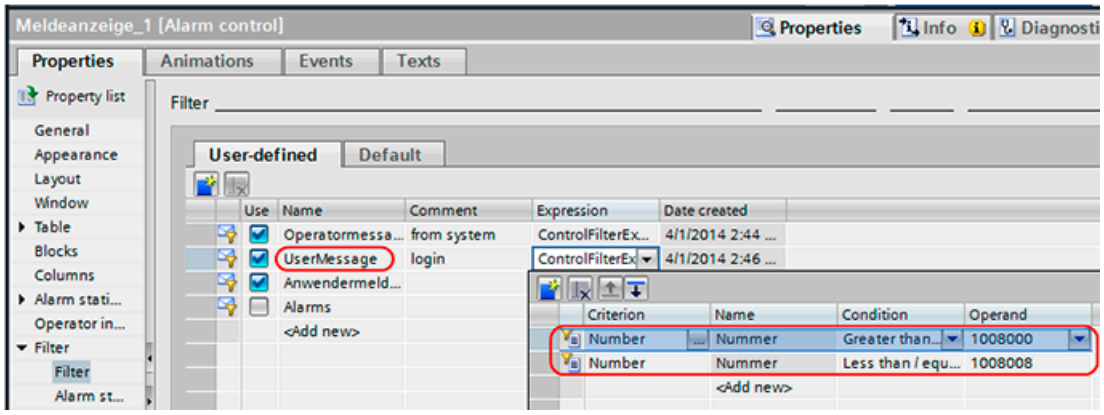


The system alarms must be created in the "System events" tab in the "HMI alarms" editor before logon and logout actions can be entered in the alarm system. The import dialog opens when the tab is selected for the first time (see figure below).



For the display of the operator input alarms, the "Alarm view" is moved from the Tools > Controls area to a process screen using drag-and-drop. So that only operator input alarms and logon/logout actions are displayed in the "Alarm view", the corresponding filters must be set.

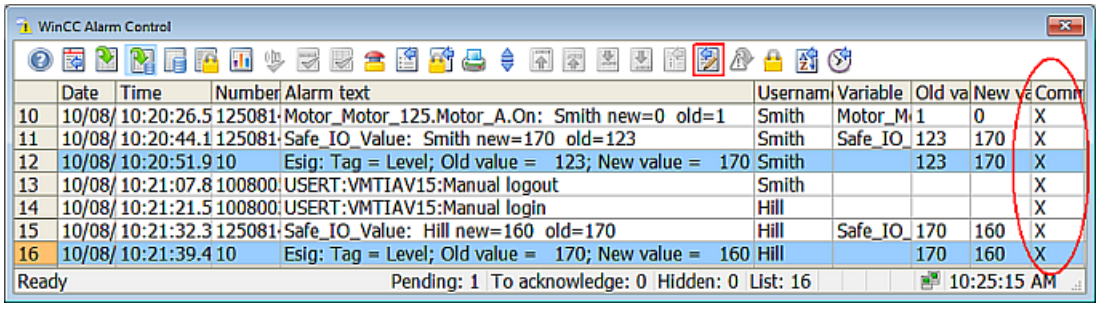




User-defined user alarms can be filtered according to the alarm number as well.

So that logons via a web connection are also displayed, a filtering according to the alarm numbers 1012400 and 1012401 must also be provided.

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



The icon in the **Comment** column indicates that a comment is present. This can be displayed using the button marked in the screenshot.

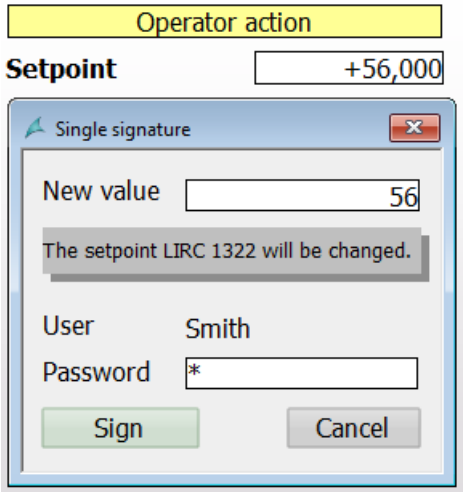
6.5 Configuration for electronic signature

In order to use electronic signatures in a computer system instead of handwritten signatures, legal regulations such as 21 CFR Part 11 of the U.S. FDA and Annex 11 of the EU GMP Guide must be complied with. Other laws and regulations or the process owner define for which actions signatures are required. The owner of the process always decides which of these signatures may be carried out electronically.

Operator actions in WinCC, such as inputs using I/O fields or buttons, can be configured such that a single electronic signature is requested from the logged-on user.

Example: A setpoint is to be changed. When the I/O field is clicked, a screen window appears in which the logged-on user signs electronically by confirming his password. Only then is the setpoint change carried out. During this operator action, a script with the VB function *VerifyUser* or *AuthenticateUserNoGUI* is called in the background and activates the SIMATIC Logon Service. The function authenticates the logged-on user using the password entered. The electronic signature is established by an audit trail entry via the call of a user alarm, see chapter "Audit trail (Page 102)".

The screen window for the electronic signature can be flexibly designed. During operation, the electronic signature information could look like this:



6.6 Recipe control

6.6.1 WinCC Recipes option

The creating of database tables with multiple data records in the "Recipes" editor can be configured such that the GMP requirements for the audit trail of parameter data (recipe data / machine data) are complied with.

For this purpose, I/O fields are created in a recipe screen and linked to the respective data fields. If the "Operator input log" property is activated for the I/O field, the entry of a value triggers an operator input alarm.

See also

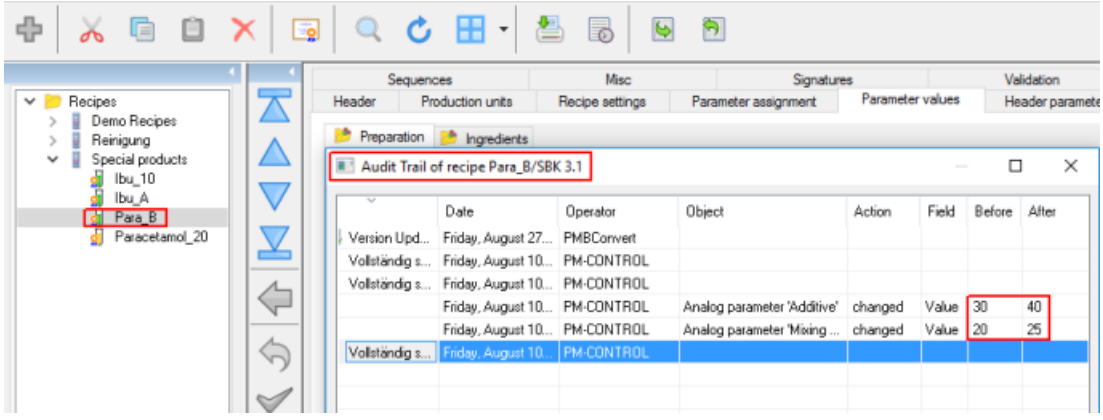
- TIA Portal Information System > Visualize processes > Working with recipes
- TIA Portal Information System > Visualize processes > Working with system functions and Runtime scripting > Reference > Events > Overview (RT Professional) > Elements (...)

6.6.2 WinCC Premium Add-on PM-CONTROL

WinCC Premium Add-on PM-CONTROL provides easy, straightforward maintenance of recipes, see also chapter "WinCC Premium Add-ons (Page 37)" - Batch-based control with PM-CONTROL.

PM-CONTROL manages recipes or machine data records in a separate database. The following functions are supported:

- Change tracking in a separate recipe-related audit trail
- Automatic versioning of the recipes
- Electronic signature for input as well as for changes in the recipe data records, only fully signed recipes are available for production.
- Restoration of an older recipe version using an integrated mechanism
- Configurable retention period for recipes in the recipe database
- Various states for recipes



See also

- PM-CONTROL system description at (http://www.siemens.com/process-management)
- Chapter "WinCC Premium Add-ons (Page 37)"

6.7 Electronic data recording and archiving

It is very important to provide complete quality evidence with regard to quality-relevant production data, especially for production plants operating in a GMP environment.

Multiple steps must be performed for electronic recording and archiving:

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

6.7.1 Specifying the data to be archived

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

- Definition of the data from different origins that must be archived, such as process values, alarms, batch data, reports, audit trails, log files etc.
- Definition of the respective recording cycles
- Specification of the respective storage duration, online and offline
- Definition of the archiving cycle for external export

This data is stored in various archives:

- Data logs
- Alarm log
- PM-QUALITY database
- PM-CONTROL databases

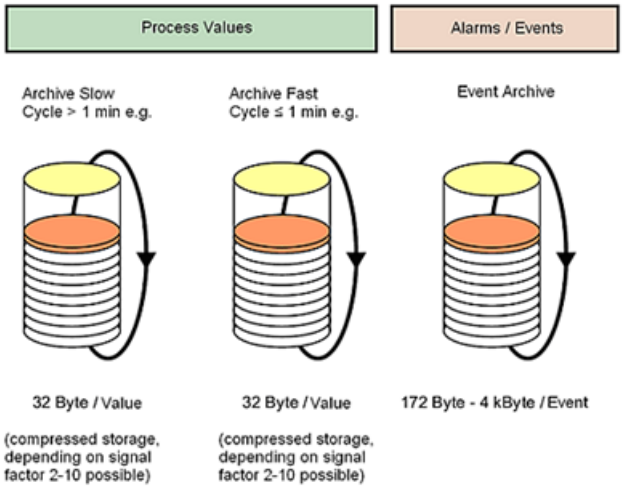
Actions are also monitored and recorded in log files or databases in other parts of the system:

- WinCC reports
- SIMATIC Logon EventLog
- Event Viewer under Windows Computer Management (logon/logoff activities, account management, rights settings for the file system, etc., according to the corresponding configuration)

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

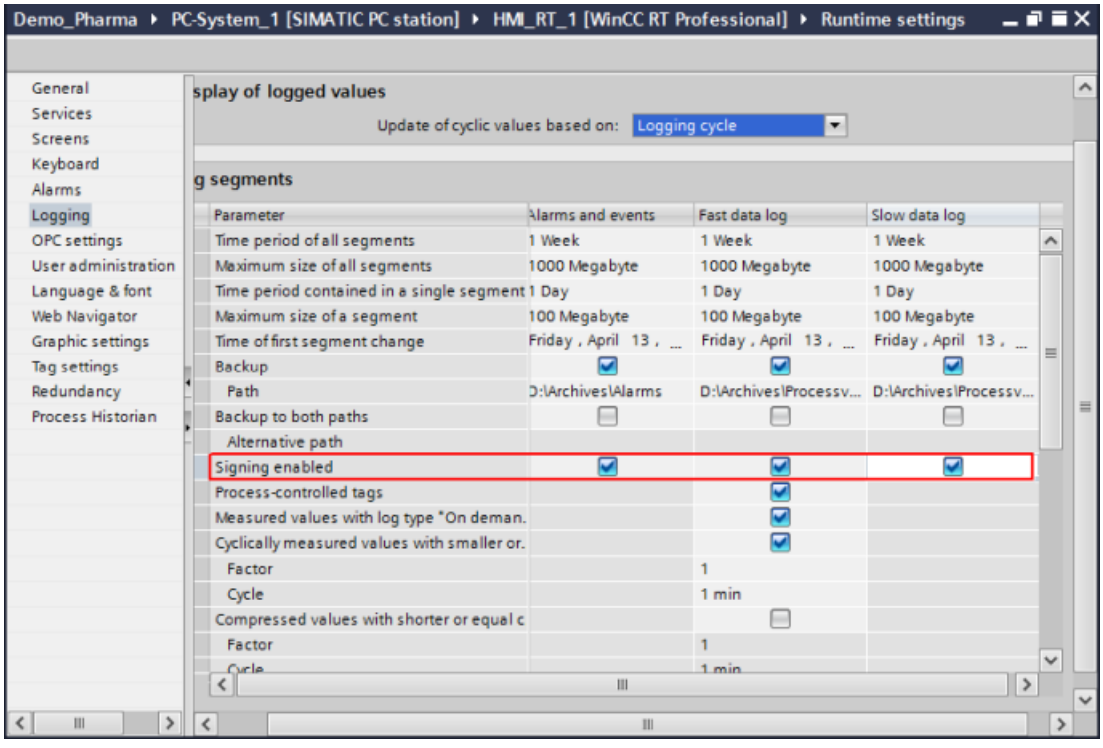
6.7.2 Recording and archiving

Archiving in WinCC takes place in two steps. Messages and process values are first recorded in individual segments in the alarm log and in the data log as circular log.



These short-term archives can be backed up in a long-term archive using a variety of solutions and stored there for the time period defined by the customer.

Data recording in SIMATIC WinCC

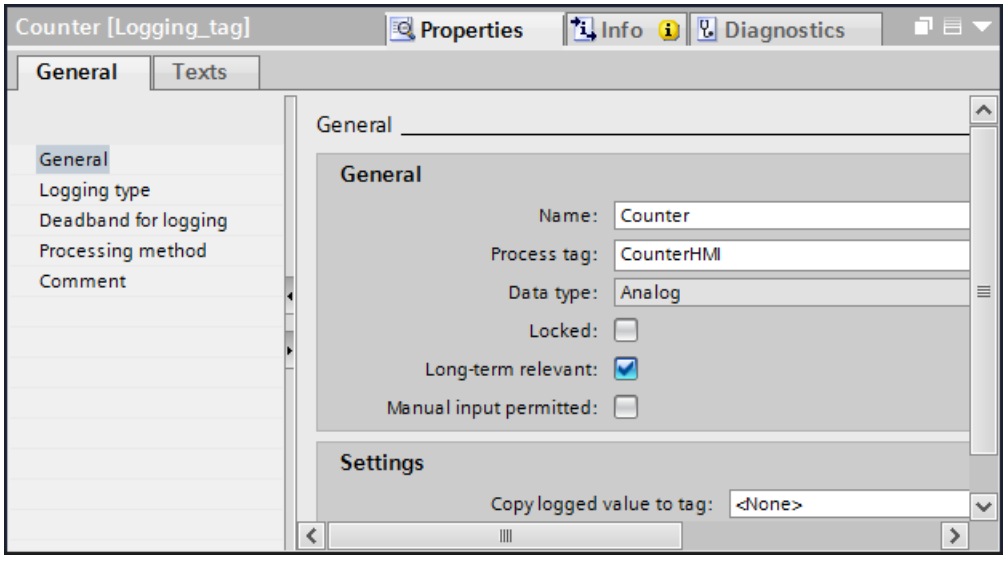


For the archiving of alarms and process values in the GMP environment, the size of the circular logs (time period of all segments) and the size of the individual segments are defined in the Editor runtime settings under logging.

Long-term archiving (swapping out of the archives)

To secure the archived data in the long term, the backup functions are activated for all log types and a path is specified for swapping out the archived data. The archive data is saved in database format. By selecting the property "**Signing enabled**", an internal algorithm forms a checksum when swapping out. Through this, the system recognizes subsequent manipulations and these are indicated when a connection is established to a manipulated database.

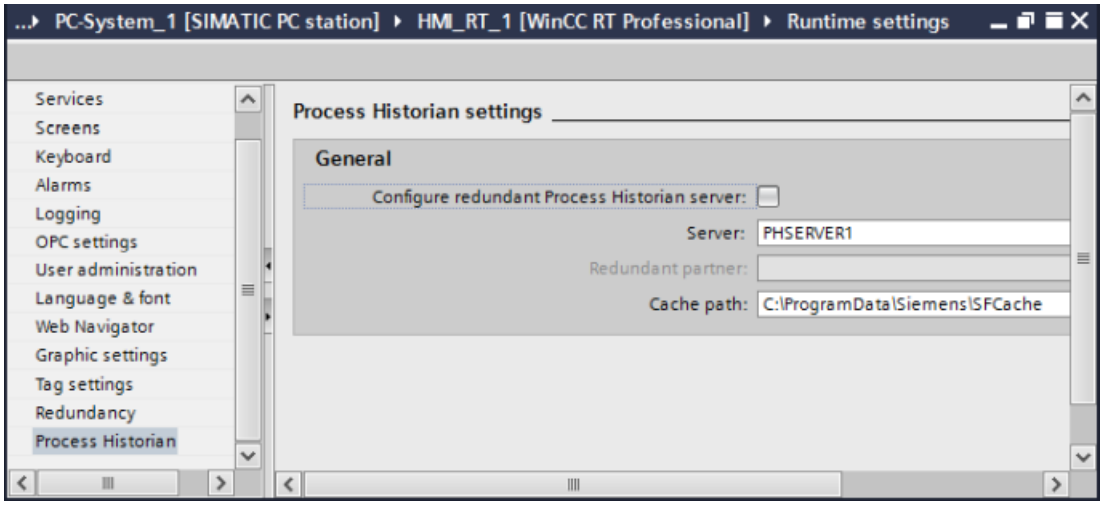
The alarm log is generally swapped out. Process logs only swap out those tags for which the "long-term relevant" property has been activated.



The WinCC DataMonitor option, for example, can be used to view the swapped-out data.

SIMATIC Process Historian

The WinCC option SIMATIC Process Historian archives process values and messages from one or more operator systems of the WinCC, WinCC RT Professional and PCS 7 type in a central database. The number of connected systems, including redundant systems, is not limited. All the messages stored in the WinCC archives are transferred to the Process Historian. Only those tags are accepted for which the "long-term relevant" property is activated. After installing the Process Historian option, activation can be made in the "Runtime" editor.



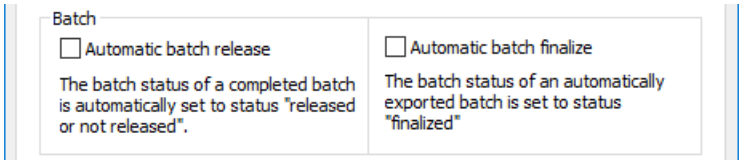
See also

- "Process Historian 2014 SP3" manual, Online Support under entry ID 109762798 (https://support.industry.siemens.com/cs/ww/en/view/109762798)
- Trend Viewer for the SIMATIC Process Historian 2014, Online Support under entry ID 109756715 (https://support.industry.siemens.com/cs/ww/en/view/109756715)

6.7.3 Archiving batch data with PM-QUALITY

In PM-QUALITY, the acquired batch data can be exported manually or automatically in database, HTML or XML format. The acquisition of the data is described in chapter "Batch-based reporting with PM-QUALITY (Page 112)".

Only completed batches can be archived. Selecting the "Complete automatically" check box in the Project settings > Defaults dialog has the effect that changes/additions to the batch data are no longer possible after the automatic export in database format.



For export in HTML or XML format, the subsequent manipulation of the data can be prevented through corresponding rights on the drive (read only) or through automatic conversion to PDF format using auxiliary tools.

See also

- PM-QUALITY system description at (http://www.siemens.com/process-management)

6.7.4 Increased availability for data archiving

PM-QUALITY Professional with Data Center can be used for the continuous recording of batch data in a redundant system with two WinCC RT Professional servers. A precondition for this is that the computers are time-synchronized.

Upon completion and release of a batch, the Application Data Center merges the recorded batch data from two PM-QUALITY runtime databases into one export database. If one WinCC server is not available, the Data Center only becomes active when both WinCC servers are operating again.

6.8 Reporting

6.8.1 Reporting of process and production data

The documentation of process and production data is configured in the "Report" editor. The following data, among others, can be recorded:

Alarm sequence report	Chronological listing on a line printer of all messages occurring since the start of WinCC Runtime
Alarm report	Alarms of the current alarm list
Log report	Alarms from the alarm log, e.g. audit trail based on operator input alarms
Tag table	Tag contents from process value logs or compressed logs in the form of a table
Tag trend / screen	Tag contents from process value logs or compressed logs in the form of a trend
Recipes	Data records of recipes in tabular form
Hardcopy	Hardcopy of screen contents
Tag values	Current process values at defined times

Note

WinCC reports support reporting based on continuous archives.

The layouts for reporting are designed according to the requirements of the specification. In addition to detailed pages of content, a report may also include a front page, rear page and a header and footer. There are numerous tools available for displaying the content. These can be easily moved into the detail area using drag-and-drop and then configured.

See also

- TIA Portal Information System > Visualize processes > Working with reports

Print jobs

For the output of a report on a printer, a print job is defined in which the report name, time range, page range and the printer are specified. The print job can be started as a time-controlled or event-driven job.

The output of the audit trail entries is shown in the report as follows:

Audit Trail

	Date	Time	User nar	Meldetext	OldValue	NewValu
1	13/08/	13:00:07.570	Hill	Motor_Motor_125.Motor_A.On: Hill new=1	0	1
2	13/08/	13:00:05.665	Hill	Motor_Motor_124.Motor_A.On: Hill new=1	0	1
3	13/08/	12:59:54.858	Hill	Safe_IO_Value: Hill new=285 old=290	290	285
4	13/08/	12:59:43.949	Hill	USERT:VMTIAV15:Manual login		
5	13/08/	12:59:14.338	Smith	USERT:VMTIAV15:Manual logout		
6	13/08/	12:59:03.229	Smith	Motor_Motor_125.Motor_A.On: Smith new=	1	0
7	13/08/	12:59:01.123	Smith	Motor_Motor_124.Motor_A.On: Smith new=	0	0
8	13/08/	12:58:34.101	Smith	Safe_IO_Value: Smith new=290 old=123	123	290
9	13/08/	12:58:13.424	Smith	Motor_Motor_231.Motor_A.On: Smith new=	0	1
10	13/08/	12:58:09.245	Smith	Motor_Motor_124.Motor_A.On: Smith new=	1	0

6.8.2 Batch-based reporting with PM-QUALITY

The WinCC Premium Add-on PM-QUALITY is used for batch-based acquisition 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 with a unique name, which can be configured, and can be called again using the batch name.

Over the time range of the batch run time, the process values are recorded in the separate PM-QUALITY database, staggered according to different acquisition cycles, or are transferred from the WinCC data logs. Event-driven or trigger-dependent process values (e.g. setpoints, actual values) are recorded as a snapshot. Alarm events and audit trail entries are transferred from the alarm logs (Panel and WinCC RT Advanced) or the HMI alarms (WinCC RT Professional) to the PM-QUALITY database.

See also

- PM-QUALITY system description (http://www.siemens.com/process-management)

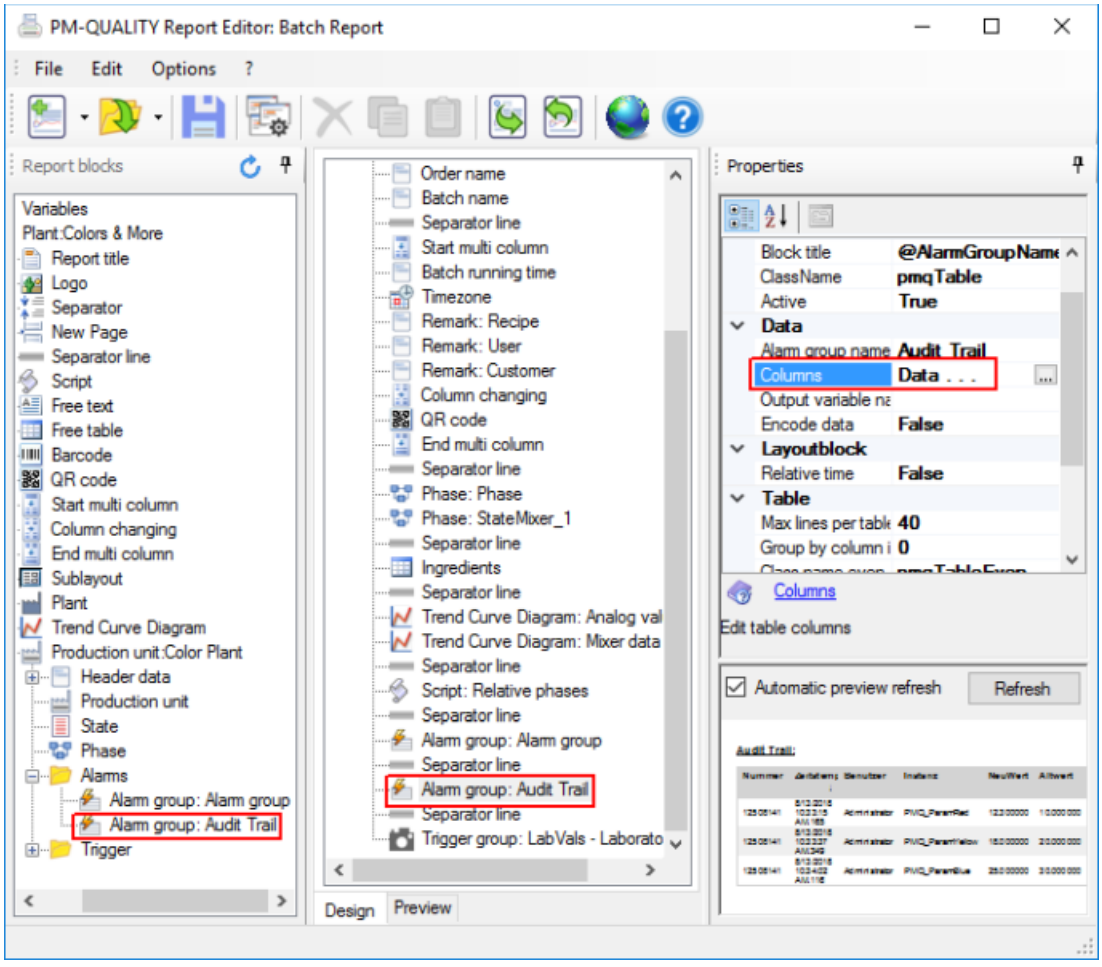
PM-QUALITY Design of the batch report

The report editor provides numerous options for a user-defined report layout for the batch report.

An example of how to display audit trail entries (operator input alarms) in a batch report is explained below.

The alarm blocks to be displayed in the batch report are selected in the properties of the Audit Trail alarm group in the Topology Manager. Next, the alarm number for the operator input alarm defined in the WinCC system is entered in the alarm filter dialog.

The Audit Trail alarm group is displayed in the report editor under available report blocks. The audit trail alarm group is moved to the right using drag-and-drop for display in a report layout. The display is defined in the properties for the report block.



The display of an audit trail in a batch report can have the following appearance:

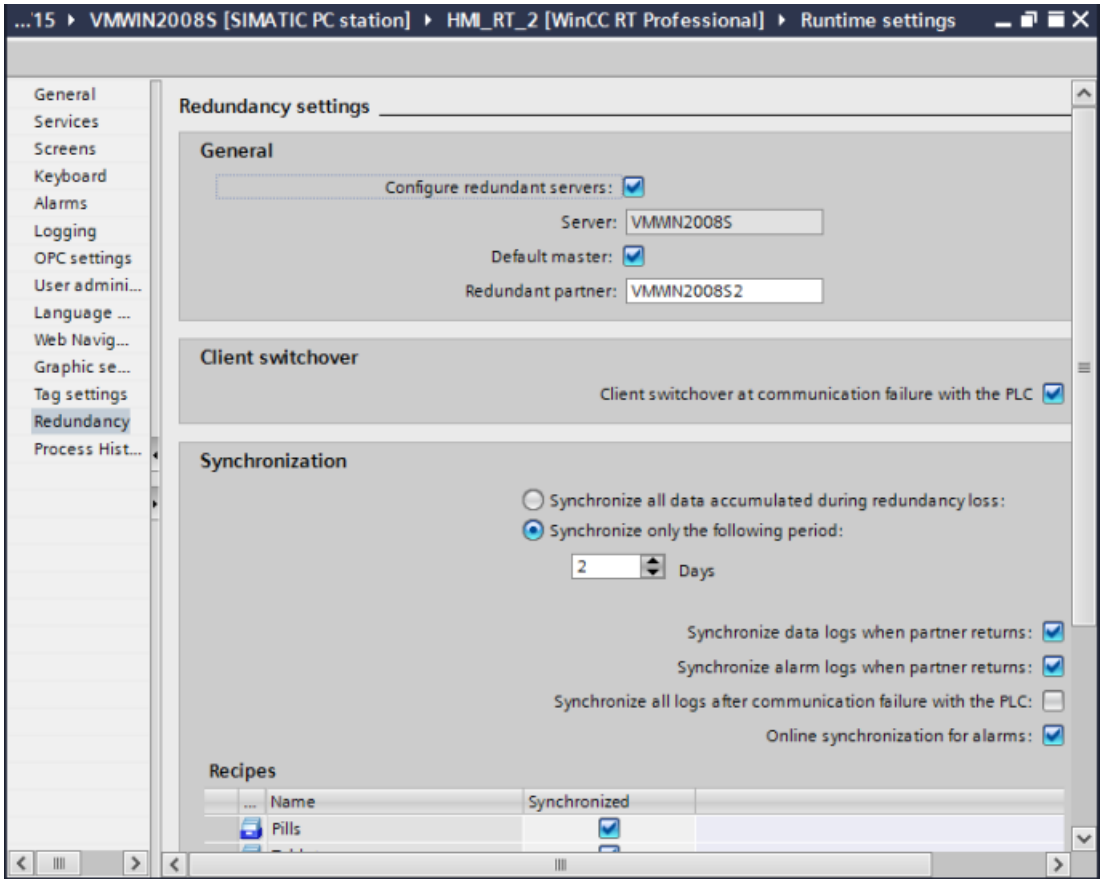
AuditTrail:

Number	Timestamp	User	Instance	OldValue	NewValue	Comment
12508141	8/30/2018 1:15:33 PM.603	Administrator	PMQ_ParamRed	10.000000	15.000000	More red paint
12508141	8/30/2018 1:15:46 PM.040	Administrator	PMQ_ParamYellow	20.000000	18.500000	Less yellow paint
12508141	8/30/2018 1:16:03 PM.255	Administrator	PMQ_ParamBlue	30.000000	27.000000	Blue paint adaption

Change comments can be displayed directly in the audit trail.

6.9 Redundant system

The WinCC RT Professional operating system features the redundancy option. Setting up a redundant operating system significantly increases availability. The WinCC servers monitor each other and automatically synchronize the data after a failure. The WinCC clients automatically connect to the active server. This ensures the monitoring and operation of the process.



In addition to activating the "Redundancy" property, the configuration dialog also contains settings for adjusting the data.

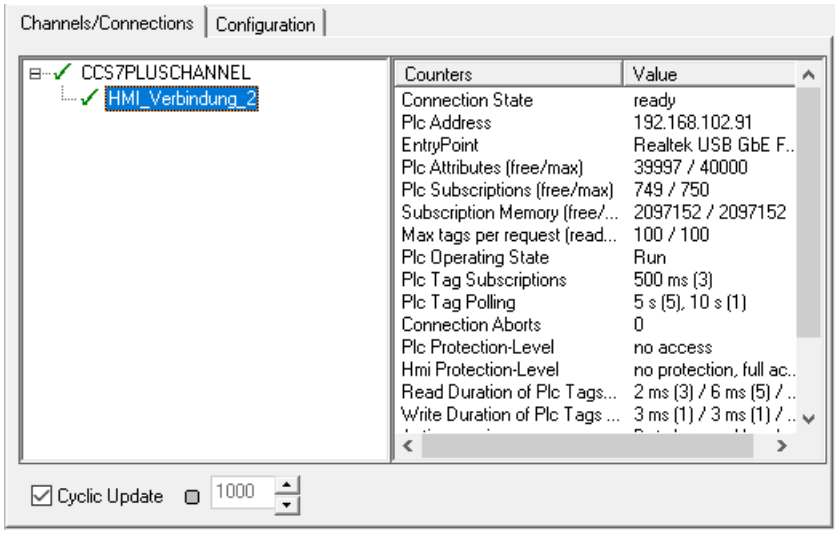
See also

- TIA Portal Information System > Visualize processes > Options > WinCC redundancy

6.10 Monitoring of the system

6.10.1 Diagnostics of communication connections

WinCC provides the Channel Diagnostics application for monitoring communication connections to the secondary controllers. The application can be opened using Start > All programs > Siemens Automation > Runtime Systems or integrated in a WinCC screen (e.g. diagnostic screen) as an ActiveX Control. The status of the channels that support diagnostics is displayed in a window. Information on the start / end of the connection, version ID and error alarms with time stamp are recorded automatically in a log file. In this way, evidence regarding the quality of the communication connections is provided by the system.



6.10.2 Memory space view

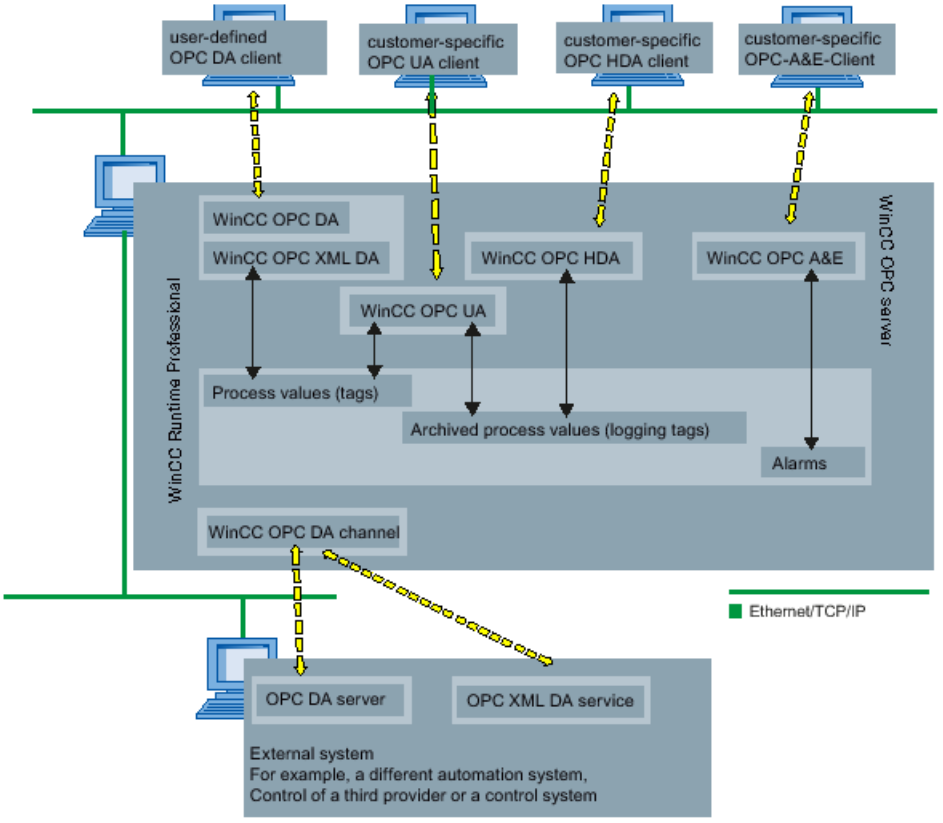
The DiskSpaceView object displays, in the form of bar, the percentage of the total memory capacity of a drive that is used. For monitoring purposes, a memory space display can be integrated in a screen (e.g. diagnostic screen) for each drive. Percentages and bar colors can be configured for tolerance, warning and alarm.

6.11 Data exchange with the plant control level

Data exchange with the plant control level or other systems must be covered by system functionalities. Various methods are available for this purpose. For access to archive data and process tags, OPC interfaces are available that can be installed with the system software. Other methods for direct access to the archive databases are available with ADO / OLEDB or via Runtime API.

The following interfaces are included in the scope of delivery:

- WinCC OPC DA / OPC XML DA
- WinCC OPC Historical Data Access (HDA)
- WinCC OPC Alarm and Events (A&E)
- WinCC ADO/OLE DB
- WinCC OPC UA (Data Access and Historical Data)



See also

- TIA Portal Information System > Visualize processes > Interfaces > OPC for Runtime Professional
- TIA Portal Information System > Visualize processes > Working with alarms > Alarm logging > Configuring alarm logging (RT Professional)

Data exchange via Runtime API

In Runtime API, the programming interface of WinCC is open. As a result, internal WinCC functions can be used and tags or archive data accessed in custom applications.

See also

- TIA Portal Information System > Visualize processes > Interfaces > Runtime API (RT Professional)

6.12 Setting up a web connection

Several WinCC options offer different possibilities for web access from a computer in the network to the user interface of WinCC.

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

The WinCC option WebUX offers a platform- and browser-independent operation and monitoring of the WinCC Runtime for mobile terminal devices.

See also

- TIA Portal Information System > Visualize processes > Options > WinCC WebNavigator (RT Professional)
- TIA Portal Information System > Visualize processes > Options > WinCC WebUX (RT Professional)
- "STEP 7 and WinCC Engineering" system manual, chapter 13.8.2.3 "Managing users for Web Client", Online Support under entry ID 109755202 (https://support.industry.siemens.com/cs/ww/en/view/109755202)

Both the operation via the web client and via WebUX are checked by SIMATIC Logon (user authentication) and WinCC user administration (runtime authorization).

Note

If operator messages are to be generated as audit trail entries when using the web client or via the WebUX connection, the standard functions can be used, see chapter "Creating operator input alarms (Page 97)". The script functions described there are only supported if SIMATIC Logon is installed on the computer.

The full range of functions is not available for viewing and operating the WinCC user interface via the Web. For the WebUX option, the functionality is much more limited than for the WebNavigator option.

See also

- TIA Portal Information System > Visualize processes > Options > WinCC WebNavigator (RT Professional) > Not supported functions
- TIA Portal Information System > Visualizing processes > Options > WinCC WebUX (RT Professional) > Supported functions

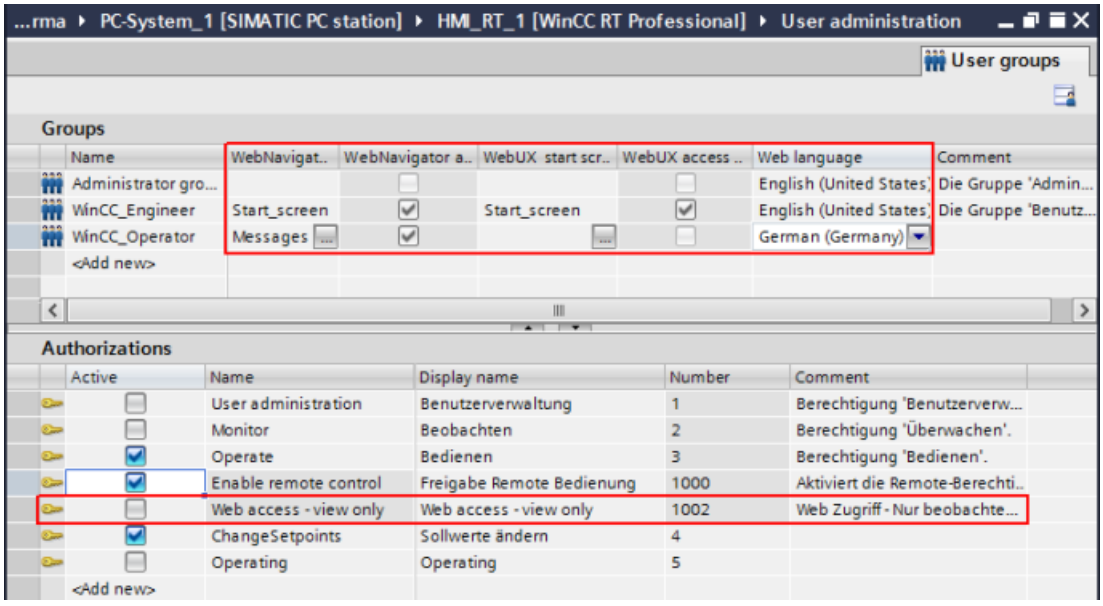
Note

For viewing process images in which ActiveX controls of the WinCC Premium Add-ons PM-CONTROL and PM-QUALITY are integrated, the respective client must be installed and licensed on the computer for the remote access.

The controls of the premium add-ons are not displayed in the WebUX view.

6.12.1 Setting up the user rights on the WinCC server

The runtime authorization in the web client and using WebUX is set up in the WinCC user administration for the user groups. If SIMATIC Logon has been activated in the Runtime settings, the user logon for both options is checked by both SIMATIC Logon (user authentication) and the User Administrator in WinCC (runtime authorization).



The respective remote accesses are activated by selecting the check box "WebNavigator access for user group" and/or "WebUX access for user group". Each option configures the web language and a start screen that is displayed when opening via web access.

Note

This configuration is carried out separately for each user group. This means that the approval for the remote access, the start page, the language, and the runtime authorization for each user group can be defined differently.

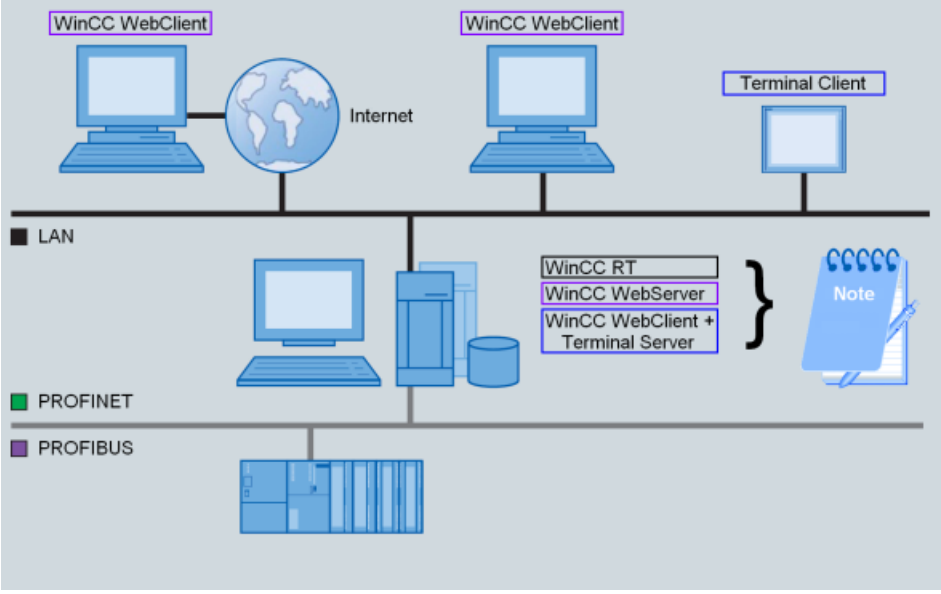
The "Web access - View only" authorization in the user administration controls the runtime authorization between WebNavigator and DataMonitor. If this function is not selected and the WebNavigator license is detected, the process screens can be operated. If this function is activated, the DataMonitor option is activated and the process screens can only be monitored.

The runtime authorization for the WebUX option is governed by the license. WebUX Operate and WebUX Monitor licenses are available. However, the activation of the "Web Access - View only" runtime authorization only permits monitoring, even if the WebUX Operate license is available.

6.12.2 Web access with the WebNavigator

The WebNavigator option can be used in two different scenarios for remote reading and writing.

- Direct connection to WebNavigator server with web clients via WinCCViewerRT
- WebNavigator server connected to terminal server via SIMATIC Thin Clients



Information and installation instructions for the two versions mentioned are compiled in an application example.

See also

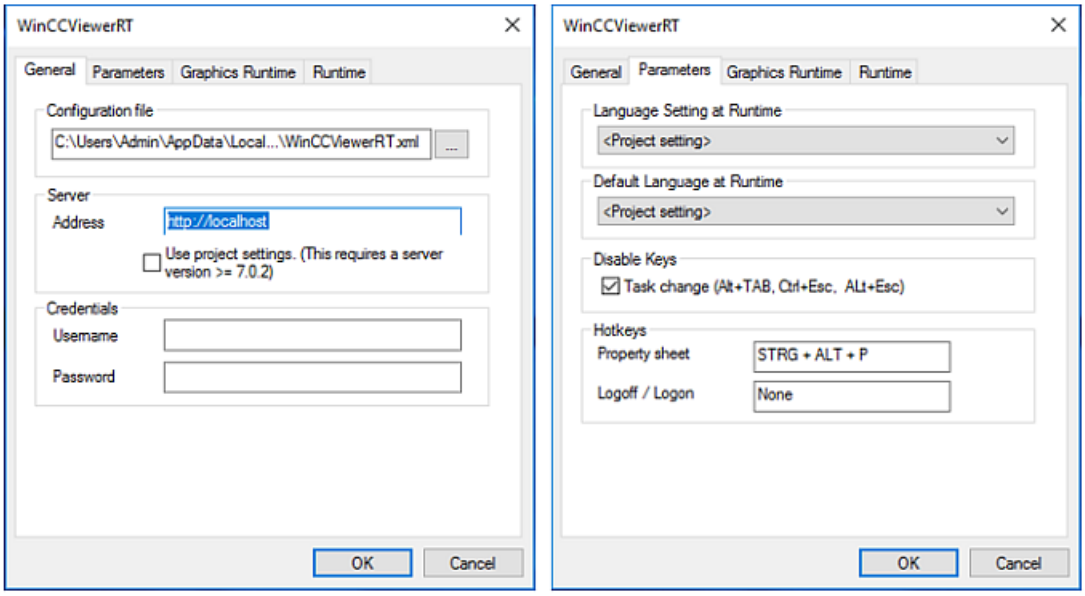
- "Documenting operator actions using WinCC WebNavigator", Online Support under entry ID 49516052 (https://support.industry.siemens.com/cs/ww/en/view/49516052)
- TIA Portal Information System > Visualize processes > Options > WinCC WebNavigator (RT Professional) > Operating a WinCC project (...)

Setting up a web client

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

The WinCCViewerRT application is automatically installed when you install a web client. Since the WinCCViewerRT can be individually configured, it is recommended that it be used instead of Internet Explorer for remote access.

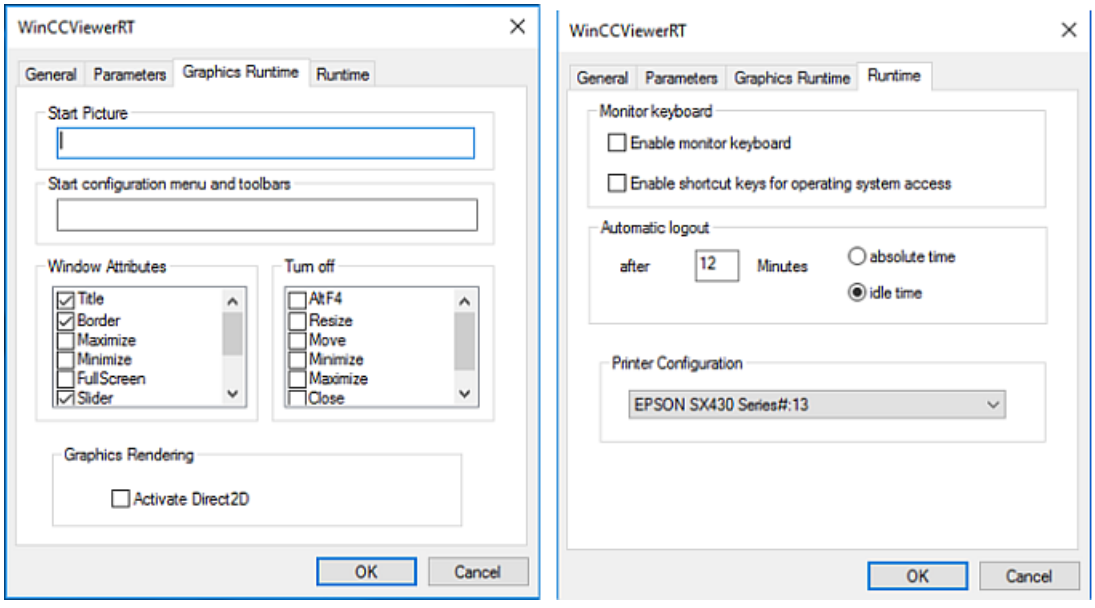
The initial parameter assignment and further application is carried out by calling the WinCCViewerRT application in the "Siemens Automation" category (depending on the operating system). Parameters are assigned the first time the application is started:



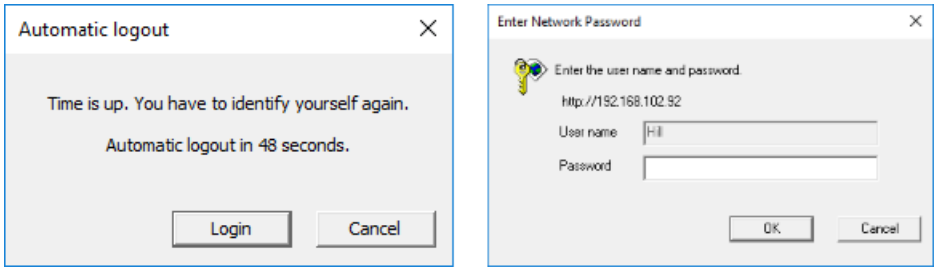
If the same user always needs to be logged in when opening WinCCViewer RT, the user data can be specified in the "General" tab. However, these fields are not filled out for the logon/logoff of different users.

A shortcut for log-on / log-off can be defined in the "Parameter" tab. This shortcut closes the current web session and opens the login dialog for entering user data again. If the logon was successful, the web view will be opened for the newly logged-on user.

The "Lock shortcut keys" property in the second screenshot should be activated.



The time configured here for the automatic logoff in the "Runtime" tab is relevant for the logoff behavior of remote access via WinCCViewerRT. In the Web view, a note about automatic log-off appears one minute before the configured time:



The settings in the configuration dialog are saved by default in the configuration file "WinCCViewerRT.xml". The connection to the web server is established when the dialog is closed via the "OK" button. The configured parameter assignments are set for additional sessions.

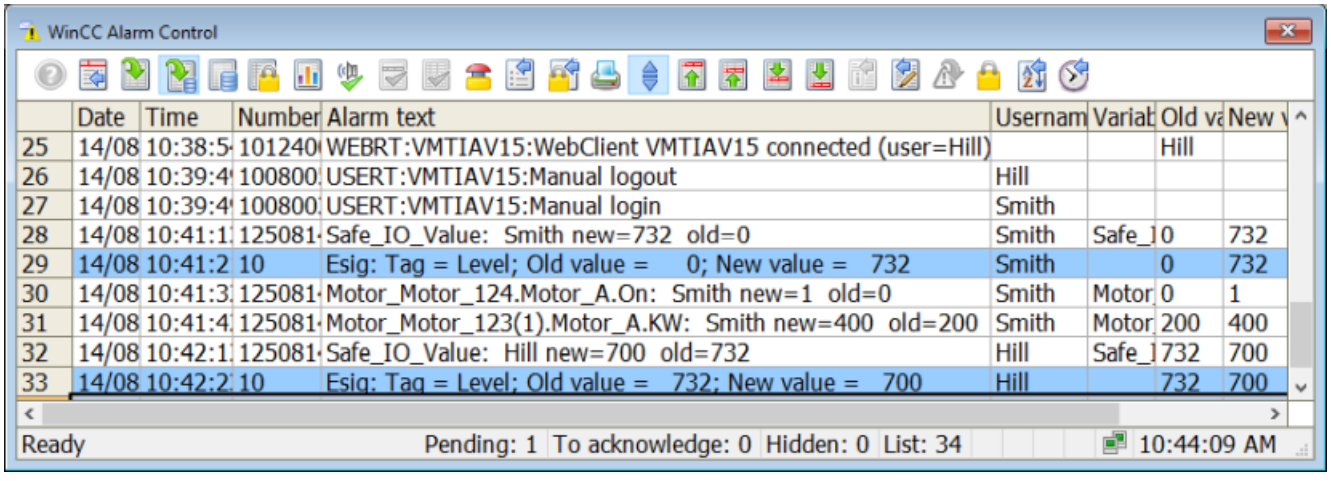
The next time the WinCCViewerRT application is started, the login dialog is opened rather than the configuration dialog. If settings need to be subsequently changed, the configuration dialog can be re-opened using the shortcut Ctrl + Alt + P. If reopening of the configuration dialog in this way is not desired for security reasons, the indicated XML file can be deleted, provided the corresponding rights have been granted. The configuration dialog will reopen once at the next start of the application.

Note

If operator messages are to be generated as audit trail entries when using the web client, the standard functions can be used (see chapter "Creating operator input alarms (Page 97)"). The script functions described there are only supported via the web client if SIMATIC Logon is installed on the computer

Logging on and off via web can be logged in the WinCC alarm logging. The system message numbers 1012400 and 1012401 are activated for this purpose. (see also chapter "Audit trail (Page 102)").

Operator actions via web access can be identified based on the entry for the computer name.



6.12.3 Web access for data display

Besides the WinCC WebNavigator option, the Trends & Alarms application of the WinCC DataMonitor option can be used to display and evaluate archived data. Trends & Alarms and the other tools available grant read-only access to the archived data.

Alternatively, the process screens with the WinCC controls show the contents of the message or data logs.

With Internet Explorer, the archive data can be displayed on any computer in the network. This requires the installation of a Microsoft SQL server on the computer where the archive databases are stored.

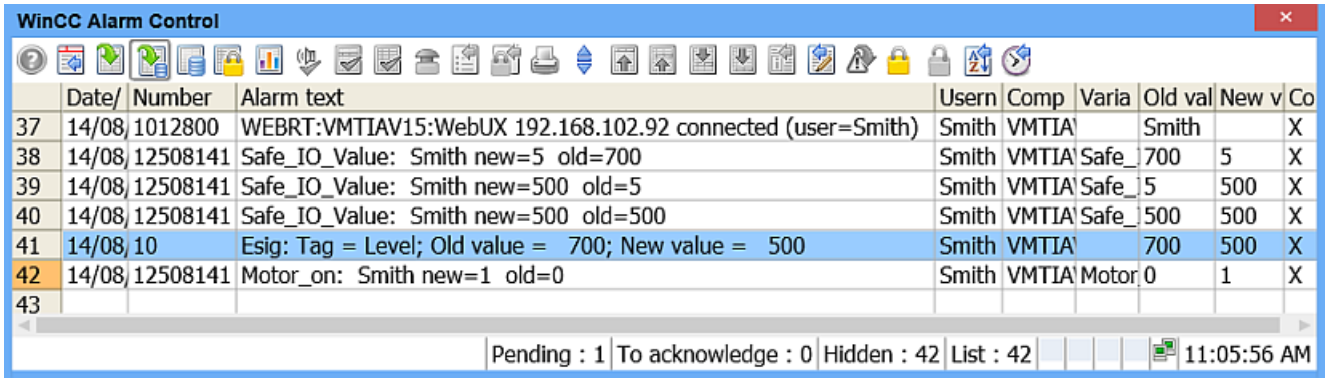
The "Archive Connector" tool is used to connect and disconnect the archived databases with Microsoft SQL Server.

6.12.4 Web access for mobile devices

Web access via the WinCC / WebUX option is based on established web standards and requires no software installation on the terminal device. Communication takes place only via a secure HTTPS connection with SSL certificates.

At the moment, this access only offers a limited functionality for the display of graphic objects and operator controls in the process screens as well as the editing of scripts.

Operator actions on objects for which the default operator input alarm has been activated, are recorded in the WinCC messages just as correctly as the simple electronic signature, see chapter "Configuration for electronic signature (Page 105)".



6.13 Interfaces to SIMATIC WinCC

6.13.1 WinCC option Control Development

WinCC Professional and WinCC Advanced provide an interface for creating user-specific complex controls. This interface is documented in detail in the WinCC ControlDevelopment option.

See also

- TIA Portal Information System > Visualize processes > Interfaces > Customer Controls (RT Advanced, RT Professional) > Overview (...)

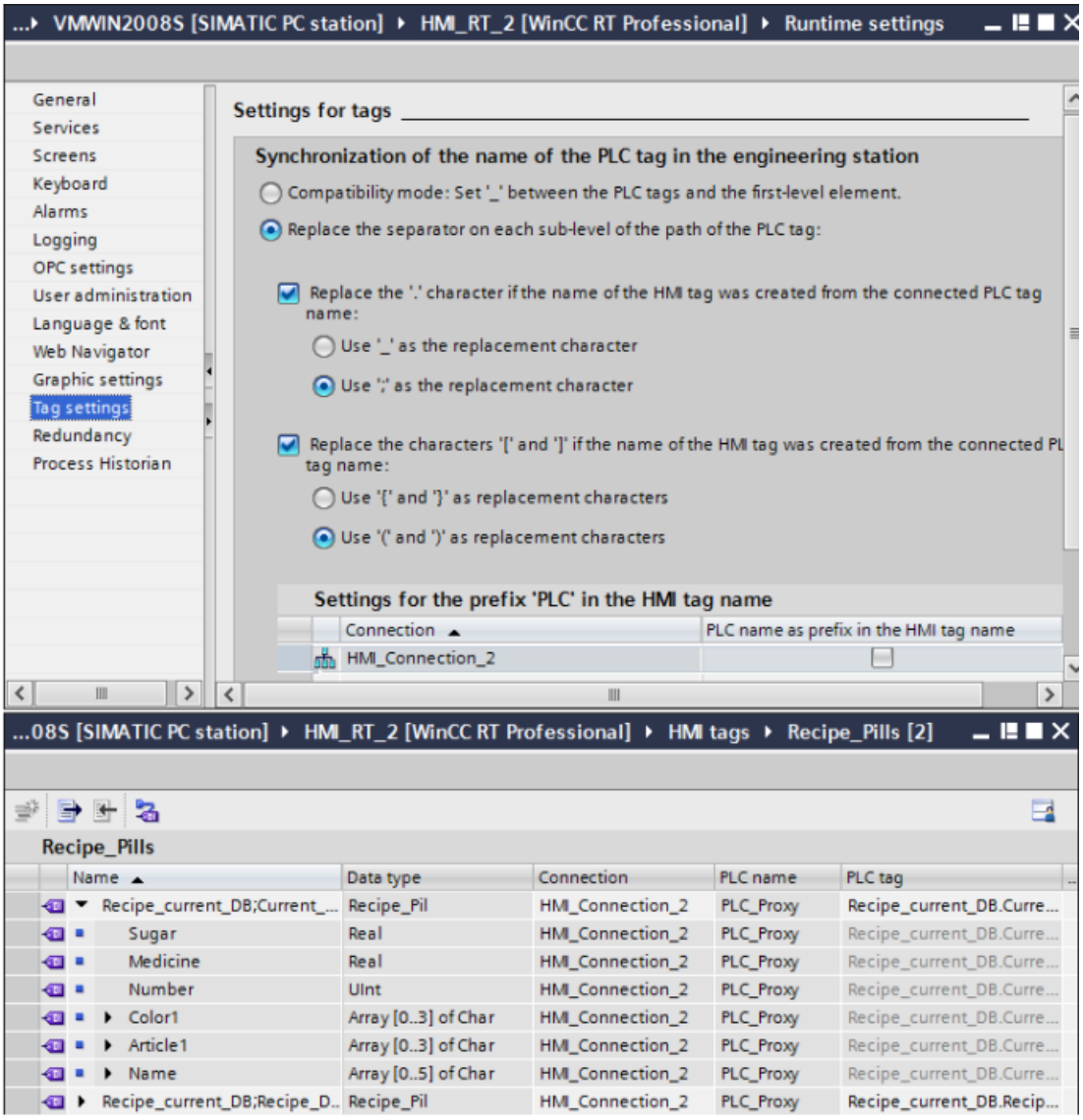
6.13.2 Connection of SIMATIC S7

Connection via defined channels

For data exchange between WinCC and the automation systems, a physical communication connection and a logical communication connection are configured in the "Devices & networks" editor.

The tag management provides the data interface between the automation system and the PC system with the WinCC RT Professional installation. All the editors integrated in WinCC read / write data in the tag management. In doing so, a direct access exists to the PLC tags (external tags), PLC data types or HMI tags (internal tags). Only PLC tags / PLC data types with the "Accessible from HMI" property allow access from the HMI device.

For the synchronization of PLC tags with PLC data types (UDT), a naming convention can be configured in WinCC. The WinCC tag names are created accordingly.



An interruption of the communication connection is displayed in the WinCC messages if corresponding system events have been enabled.

Evaluation of tag status and quality status

For monitoring purposes, 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.

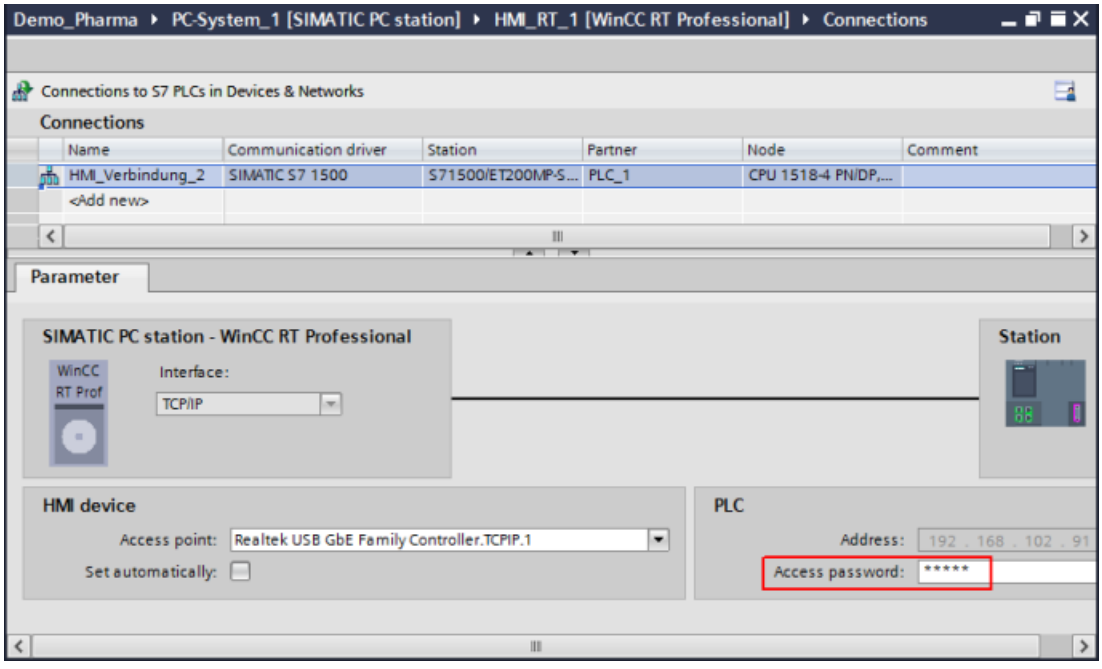
In the Inspector window, the evaluation of the tag status or the quality code for the connected process value can be configured in the property list for an object under dynamization. The evaluation is specified in a VB script.

See also

- TIA Portal Information System > Interfaces > Runtime API (RT Professional) > Data storage functions > Basics > Quality codes of HMI tags

Password for the connection establishment to the S7-1500

The data connection between the HMI device and the S7-1500 automation system can be password protected with the "HMI access" protection level. The password is defined in the CPU, see chapter "Protection functions in the automation system (Page 160)". The same password must also be specified in the project data of WinCC RT Professional when connecting to the CPU. Together with the project data, this is encrypted and downloaded to the target system. A connection between WinCC RT Professional and PLC is only established if the configured passwords in both devices match.



Password for transport

The transport password protects the transfer of project data to the target system. The configured password is queried once when the data is transferred to the runtime system. If the password was specified correctly, the certificate is stored in the certificate memory and the project data is transferred to the target system.

See also

- TIA Portal Information System > Visualize processes > Compiling and Downloading > Runtime Professional> Settings for Runtime > Password protection in Runtime (...)

6.13.3 Connection to other components and third-party suppliers

Connection via defined channels

OPC (OLE for Process Control) refers to a standardized, vendor-independent interface for data exchange. OPC UA (Unified Architecture) is the further development of OPC and provides secure data exchange based on the exchange and acceptance of certificates.

The drivers for OPC UA Server and OPC UA Client are certified by the OPC Foundation and are included with WinCC RT Professional.

SIMATIC WinCC RT Professional can be used with the OPC UA server as a SCADA system (Supervisory Control and Data Acquisition) on which one or more secondary panels or HMI devices are supplied with WinCC RT Advanced tag values.

With the OPC UA client, the WinCC RT Professional visualization system is capable of receiving tag values from OPC UA servers of the SIMATIC S7-1500 control systems or from other manufacturers, see Chapter "Data exchange using OPC UA (Page 172)".

See also

- Chapter "Data exchange with the plant control level (Page 115)"
- TIA Portal Information System > Visualize processes > Interfaces > OPC > OPC for Runtime Professional (…)

Configuration for WinCC Comfort / WinCC RT Advanced

7

Operator control, monitoring and data archiving functions are covered for panels or single-station systems with WinCC Comfort or WinCC RT Advanced. This chapter describes in detail the configuration of Comfort Panels with the engineering software WinCC Comfort. The presented configuration methods can be applied to the WinCC RT Advanced engineering system.

See also

- "STEP 7 and WinCC Engineering" system manual, for example chapter 13.10 "Mobile Panels, Comfort Panels", Online Support under entry ID 109755202 (https://support.industry.siemens.com/cs/ww/en/view/109755202)
- "SIMATIC WinCC Engineering V15 – Programming reference" manual, Online Support under entry ID 109755216 (https://support.industry.siemens.com/cs/ww/en/view/109755216)

7.1 Creating the graphic user interface

Once the basic structure for the visualization has been created using the HMI device wizard, the individual process screens are created according to the requirements. Basic objects, elements and controls for the design of the screens are available in the Tools area. Essential elements for a GMP-compliant configuration are described in chapter "Object-oriented configuration for HMI devices (Page 75)".

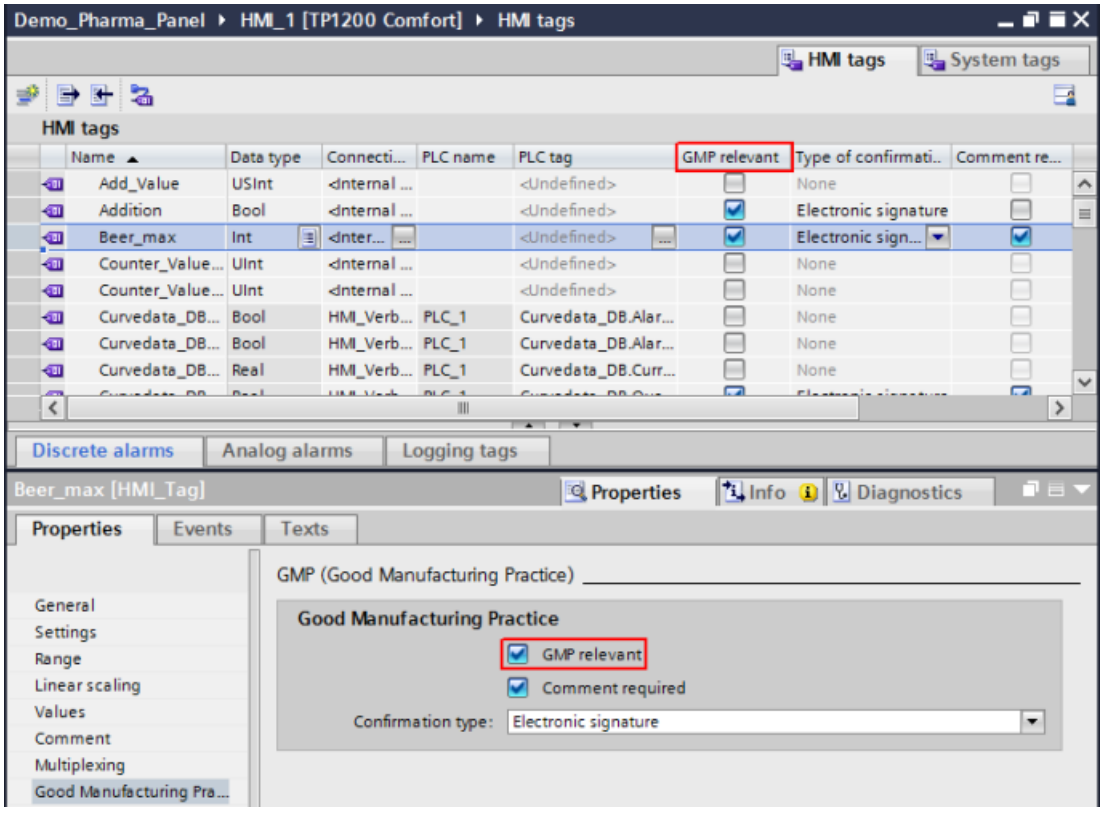
A framework design with company name, logo and buttons for screen selection can be defined in the form of templates. A template provides the basis for the process screens.

Both the process screens and the operator input philosophy must be described in the specification (for example URS, FS and P&I) and created accordingly. These should be submitted to the customer for approval in the form of screenshots.

7.2 Creating operator input alarms

For plants in the GMP environment, the international regulations, such as US 21 CFR Part 11 and EU GMP Guide Annex 11, require that operator inputs that influence GMP-relevant data be traceable. Therefore, these operator inputs must be configured such that an operator input alarm is generated. The WinCC (TIA Portal) Audit option for panels or RT Advanced support this requirement after activation of the GMP-compliant configuration (see chapter "GMP project setting in the Audit option (Page 74)"). Operator input alarms are recorded in the audit trail with time stamp, user ID, old value and new value.

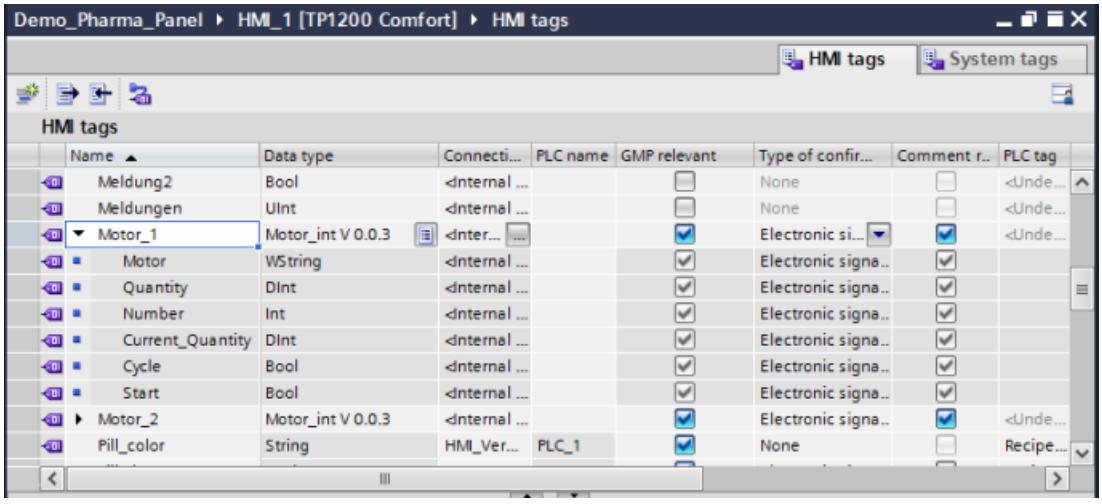
In WinCC Comfort / RT Advanced, the generation of the operator input alarm is activated for each GMP-relevant tag (not for the I/O field graphic object as in WinCC RT Professional).



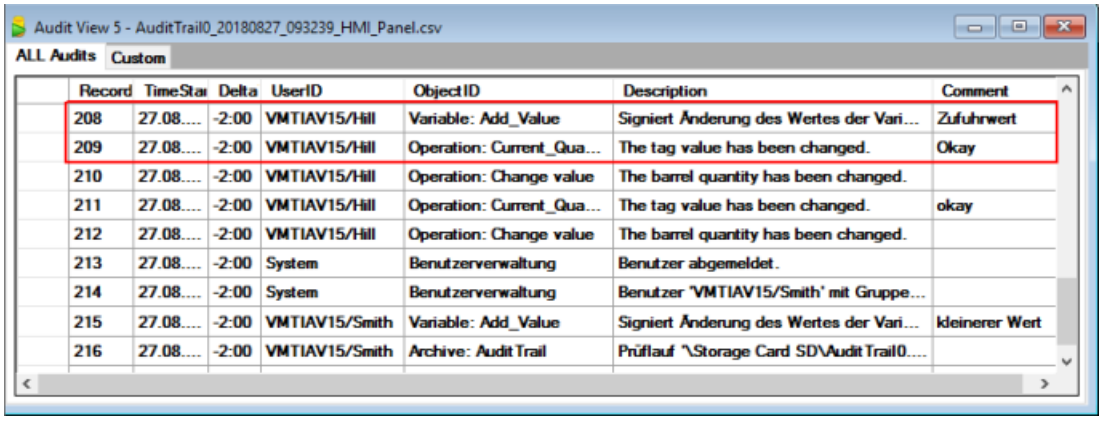
The table can be expanded to include the "GMP relevant", "Confirmation type" and "Comment required" columns using the shortcut menu for the column heading. Once the "GMP relevant" property is activated for a tag, an operator input alarm is generated in the audit trail if the value of the tag is changed (see chapter "Audit trail (Page 131)"). With "Confirmation type", the prompt for an electronic signature is set. Alternatively, confirmation can be in the form of an acknowledgement or generally omitted ("No confirmation"). If the entry is to be commented on, the "Comment required" check box is selected. For the entry of the electronic signature or a comment, a dialog is displayed automatically as soon as a GMP-relevant tag value, for example, a tag value connected to an I/O field, is changed in the operator interface (see chapter "Configuration for electronic signature (Page 134)").

Operator input alarms in combination with faceplate types

The interface of the faceplate instances is connected to tags or to tags that are an element of a user data type. For generating operator input alarms, the GMP-relevant property is activated for the individual tags in the tag table. All related elements are automatically activated as GMP relevant for a user data type (the data type Motor_int V 0.0.3 in the figure below).

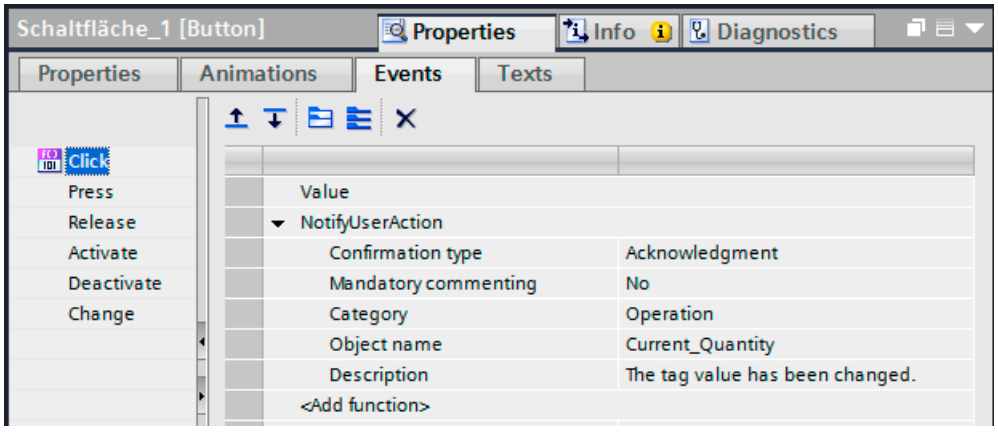


The operator input alarms are displayed as follows in the audit trail:

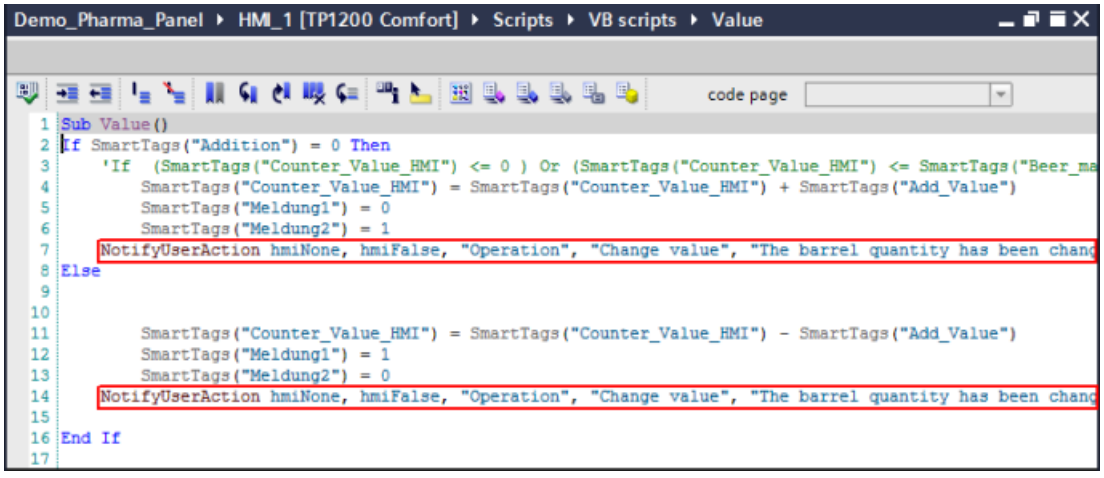


Operator input alarms with the "NotifyUserAction" system function

The "NotifyUserAction" system function can be used to generate operator input alarms for operator actions that do not directly affect a tag value, such as the pressing of a button. This is recorded in the function list at an object event ...



or integrated in a VB script as follows:



7.3 User-specific functions and scripts

Customer-specific requirements can be implemented in WinCC Comfort / RT Advanced in the form of functions or local VB scripts and then also provided with know-how protection.

See also

- Chapter "User-specific functions and scripts (Page 101)"

Such custom scripts are categorized as GAMP software category 5. The validation effort required in the form of detailed functional and interface descriptions as well as documented tests is described in chapter "Software categorization according to GAMP Guide (Page 185)".

7.4 Audit trail

When the GMP project property is activated in the Audit option (see chapter "GMP project setting in the Audit option (Page 74)"), the "Historical data" editor is expanded to include the "Audit trail" archive. The audit trail records the operator actions in chronological order thereby providing traceability of the plant operation.

The audit trail contains the following entries:

Configuration-dependent records:

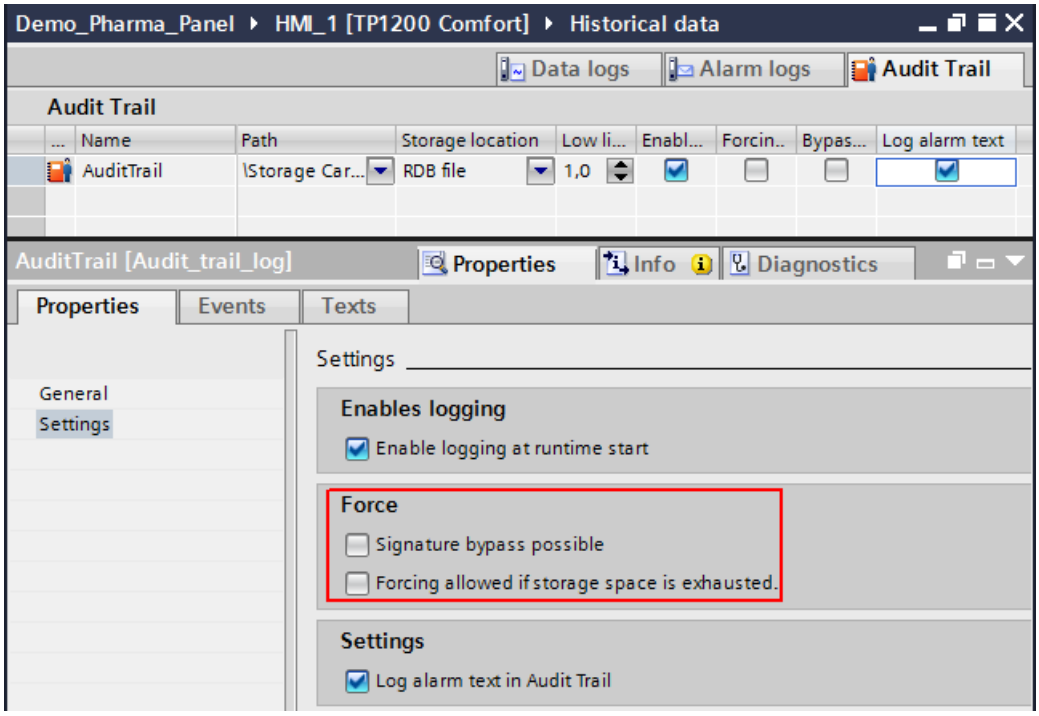
- Value change of a GMP-relevant tag
- GMP-relevant recipes, see chapter "Recipe control (Page 135)"
- Operator input alarms based on the "NotifyUserAction" system function
- Operator input alarms for operation of the alarm view (acknowledging, locking, releasing, hiding, showing)

Automatic entries without any additional configuration

- User administration
  - Logging on and off of users, including logon failures
  - Import of user administration
- Alarm system
  - All alarms that are acknowledged by the user (the alarm text can also be recorded)
  - All attempts to acknowledge
- Archive operations
  - Starting/stopping an archive
  - Opening/closing all archives
  - Deleting an archive
  - Starting a sequence archive
  - Copying an archive
- Recipe operation, see chapter "Recipe control (Page 135)"

Audit trail settings such as storage location, format and minimum storage space are made in the "Historical data" editor on the Audit Trail tab in the general properties.

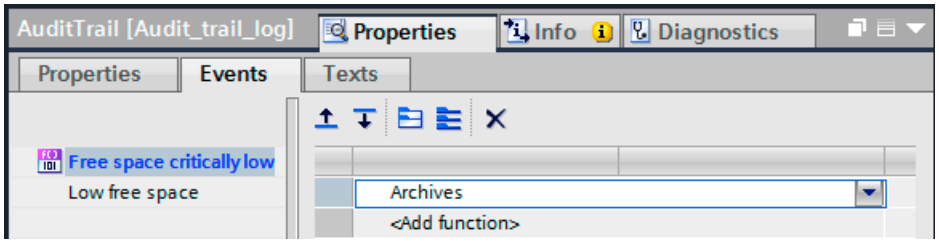
The characteristics of this archive are configured under the settings.



Note

The Force function must be deactivated in the GMP environment so that all operator messages are completely recorded in the audit trail. We recommend evaluating the events "Low free space" and "Free space critically low" and configuring a reaction in the function list. (for example, generating a warning alarm, moving the files to a network drive)

If no storage space is available, GMP-relevant operator actions are no longer feasible.



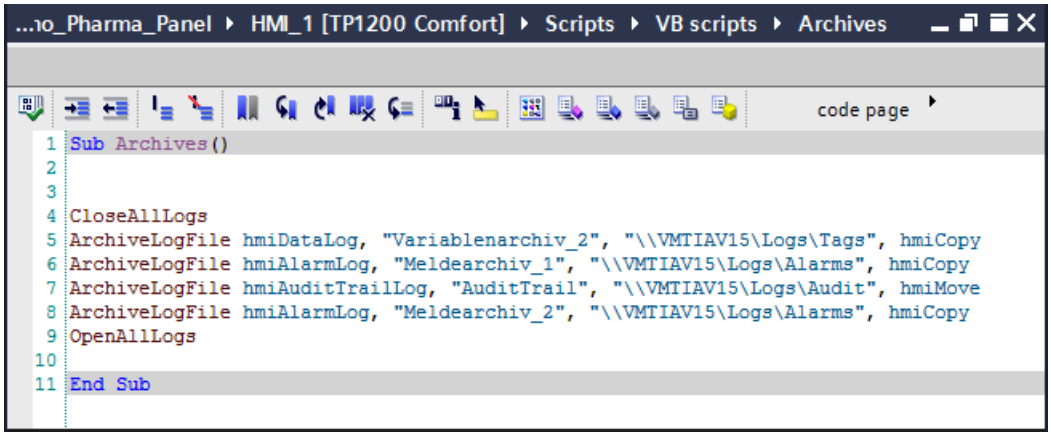
See also

- TIA Portal Information System > Visualize processes > Working with system functions and Runtime scripting > Reference > Function list > System functions (Basic Panels, Panels, RT Advanced) > Archive (...)

Displaying the audit trail

The audit trail is stored in RDB, CSV or TXT format in a circular log. A checksum, which is formed by an internal algorithm for each entry, ensures that manipulations are detected.

To view the audit trail in the Audit Viewer, the archives are closed on the HMI device, the audit trail archive is moved to another directory such as a network drive and then the archives are opened again. This is realized using a function list, or a VB script is executed via a button or the task scheduler.



The VB script shown above is a suggestion that works on small data volumes and small projects.

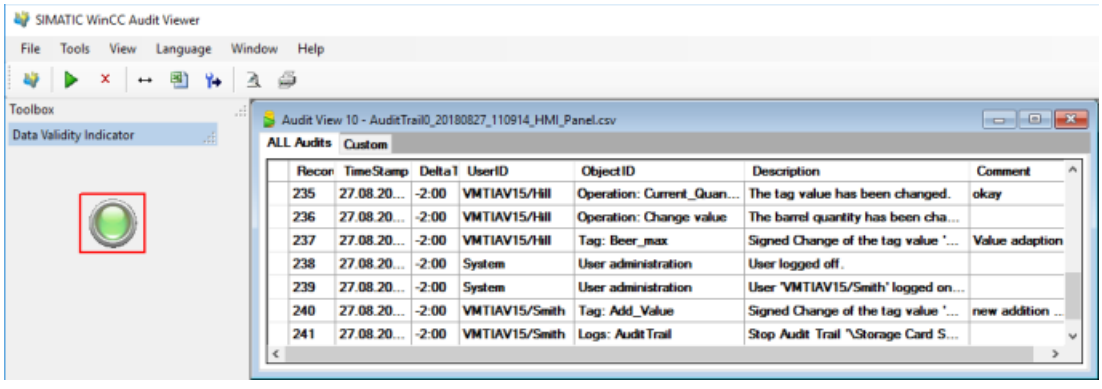
A secure method for copying or moving archives together with system events is described in the Online Support under entry ID 63042926 (https://support.industry.siemens.com/cs/ww/en/view/63042926).

See also

- TIA Portal Information System > Visualize processes > Working with system functions and Runtime scripting > Reference > Function list > System functions (Basic Panels, Panels, RT Advanced) > Archive (...)

To prevent manipulation of the audit trail files, the network drive can be protected against unauthorized access with Windows tools (see chapter "Blocking the operating system level during operation (Page 62)").

The Audit Viewer application is used for displaying the audit trail (in CSV / TXT format) on a PC and is included in the scope of delivery of the engineering system. The Audit Viewer evaluates the checksums of the entries and signals any manipulation with a red indicator and an unchanged file with a green indicator.



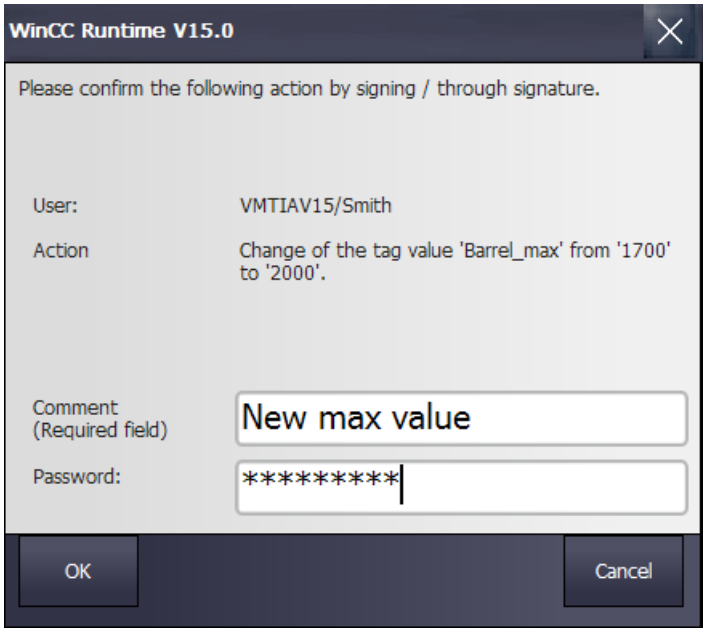
The HmiCheckLogIntegrity.exe application, which can be called in a command line or integrated in a script, provides another option for verifying the checksums in the audit trail files.

See also

- TIA Portal Information System > Visualize processes > Options > WinCC Audit (Panels, RT Advanced) > Using the audit trail (Panels, RT Advanced) > Evaluating the audit trail (...) > Evaluating audit trail with DOS program (...)

7.5 Configuration for electronic signature

A regulatory or customer-specific requirement may call for a signature for sensitive operator actions. When the "GMP" project property available in the Audit option is activated (see chapter "GMP project setting in the Audit option (Page 74)"), it is possible to configure a single electronic signature in which the logged-on user is prompted to enter the password. A dialog for entering the password is opened automatically.



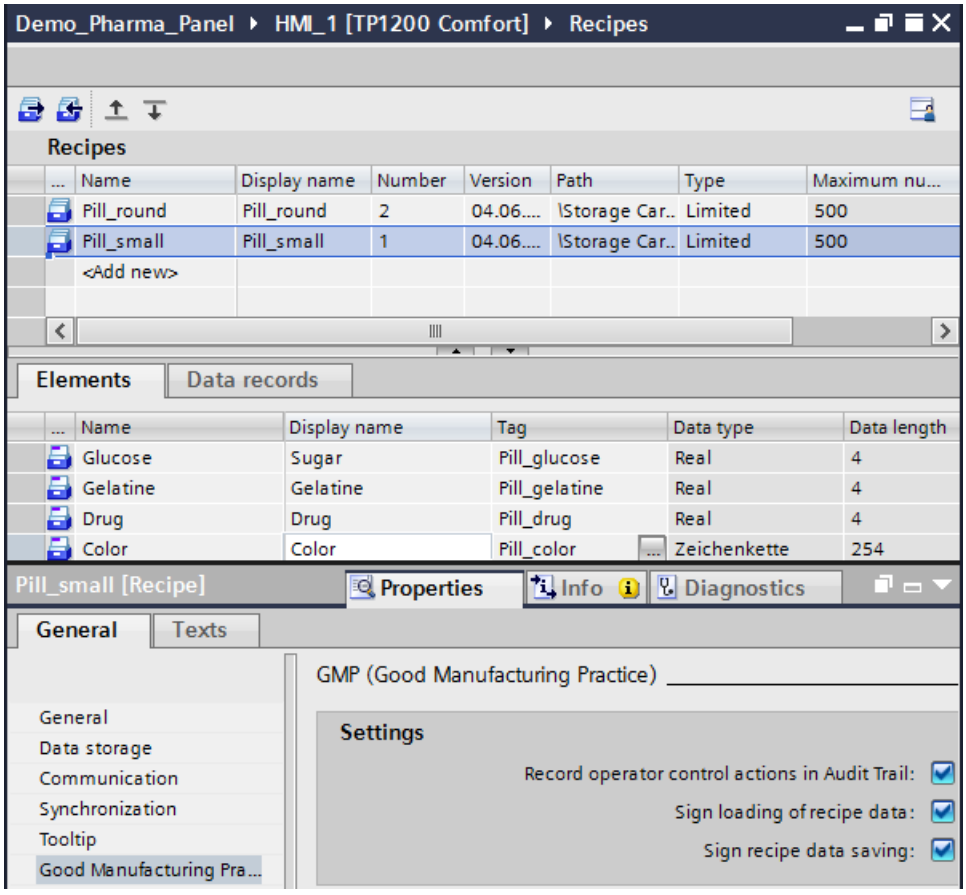
The electronic signature requirement is configured either with the tags in the tag table in the "GMP" property or with the "NotifyUserAction" system function (see chapter "Creating operator input alarms (Page 127)"). "Electronic signature" is selected as the confirmation type. If an additional comment entry is required, the corresponding check box is selected or the system function for comment required is configured with "yes".

7.6 Recipe control

7.6.1 WinCC Recipes option

Related parameters such as production data and machine parameters are summarized in a recipe. A recipe consists of several data records in which various values are stored for the individual recipe elements. Each recipe element is connected to a tag. The recipes are archived in a separate data store.

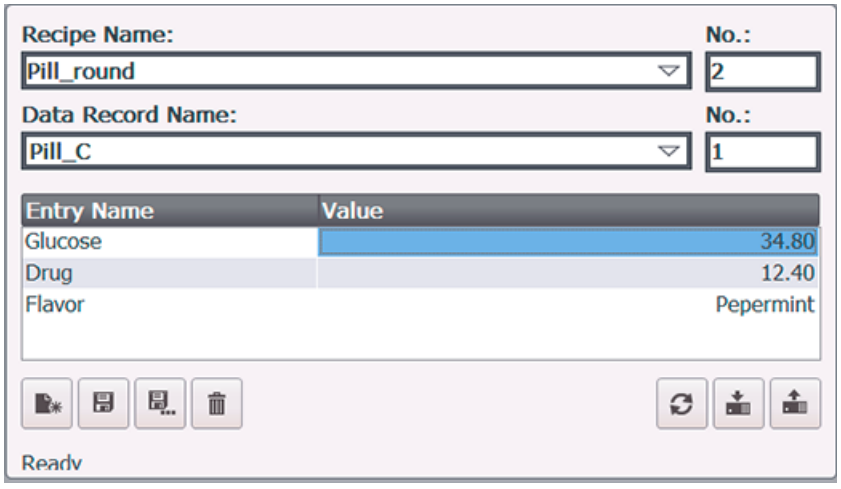
When the Recipes option is used in combination with the Audit option, GMP settings can be activated in the properties for the recipes.



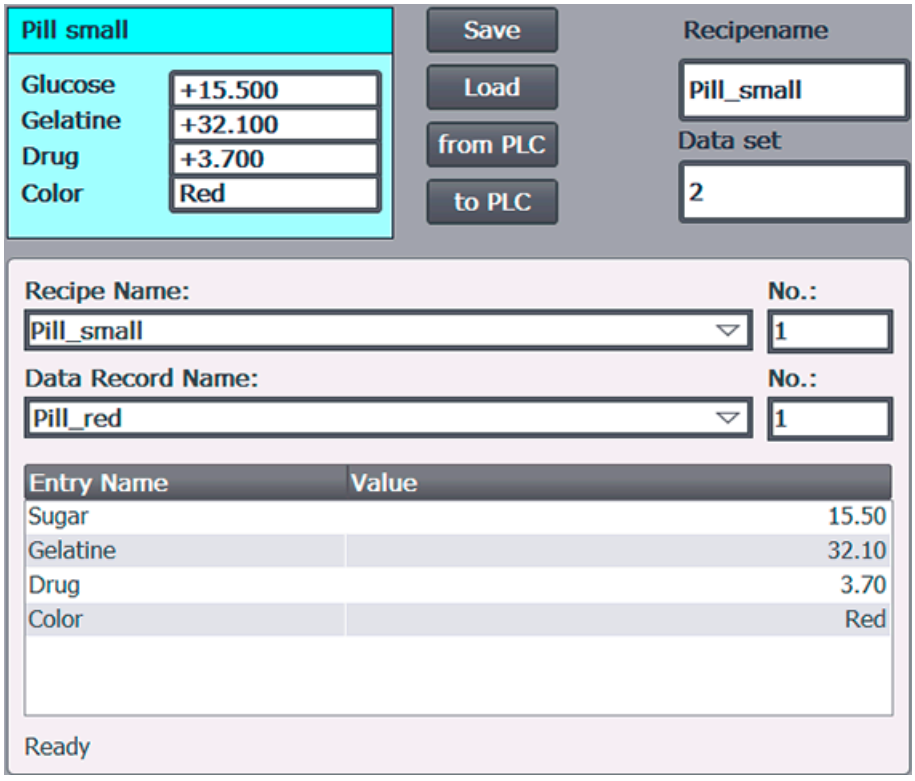
The following actions are recorded in the audit trail for GMP-relevant recipes:

- Creating and storing new recipe records
- Changing and saving recipe data records
- Transferring recipe data records to the PLC or reading from the PLC
- Changing the setting online/offline for the synchronization of tag values when using recipe tags

All recipes and data records can be displayed in the process screen with the recipe view control. A change to a data record is stored in the audit trail, but details regarding the changed values are not saved.



The recipe tags with activated "GMP-relevant" property are integrated in a recipe screen for FDA-compliant tracking of changes to the recipe data records. The recipe view control can be used for the display by deactivating the display of the toolbar buttons.



See also

- TIA Portal Information System > Visualize processes > Options> WinCC Audit (Panels, RT Advanced) > Configuring audit functions (...) > Recording recipe data changes (...)
- TIA Portal Information System > Visualize processes > Working with recipes > Working with recipes (Basic Panels, Panels, Comfort Panels, RT Advanced) > Recipes in runtime (…)
- TIA Portal Information System > Visualize processes > Performance features > General technical specifications > Memory requirement of recipes

7.6.2 WinCC Premium Add-on PM-CONTROL

WinCC Premium Add-on PM-CONTROL provides easy, straightforward maintenance of recipes, see also chapter "WinCC Premium Add-ons (Page 37)" - Batch-based control with PM-CONTROL.

PM-CONTROL is installed on a separate computer or on the computer with WinCC RT Advanced. The structure of PM-CONTROL enables the central recipe data management with automatic versioning for several production units and controllers. PM-CONTROL can be used as a standalone system for the maintenance of recipes and the management of orders. A tag connection to panels or WinCC RT Advanced or directly to an S7 controller is established via OPC UA. For the display of recipe data and the order management, PM-CONTROL provides ActiveX controls, which can be integrated into process screens with the use of WinCC RT Advanced.

The international requirements for electronic signatures according to US 21 CFR Part 11 and EU GMP Guide Annex 11 are met by PM-CONTROL, see chapter "WinCC Premium Add-on PM-CONTROL (Page 106)".

See also

- PM-CONTROL (http://www.siemens.com/pm-control)

7.7 Electronic data recording and archiving

Data recording and archiving is of great importance for production plants in the GMP environment so that complete quality evidence with regard to quality-relevant production data can be provided.

Several steps must be performed for this:

- Definition of the data to be archived, the archive sizes and the appropriate archiving strategy
- Setup of the data logs for online storage of the selected process values
- Concept for exporting the archives, for example, to a network drive

7.7.1 Specifying the data to be archived

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

- Definition of the data from different origins, such as process values, alarms, audit trails, recipe data, batch data (PM-QUALITY), etc. that must be archived
- Definition of the respective archiving cycles
- Definition of the respective retention period, both online and offline
- Definition of the cycle for the external data storage

This data is stored in various logs:

- Data log
- Alarm log
- Audit trail
- PM-QUALITY databases
- PM-CONTROL databases

Recipes are stored in the HMI device and exported to files for the data backup. The data export/ import is organized using actions, such as buttons.

Actions are also monitored and recorded in log files or databases in other parts of the system:

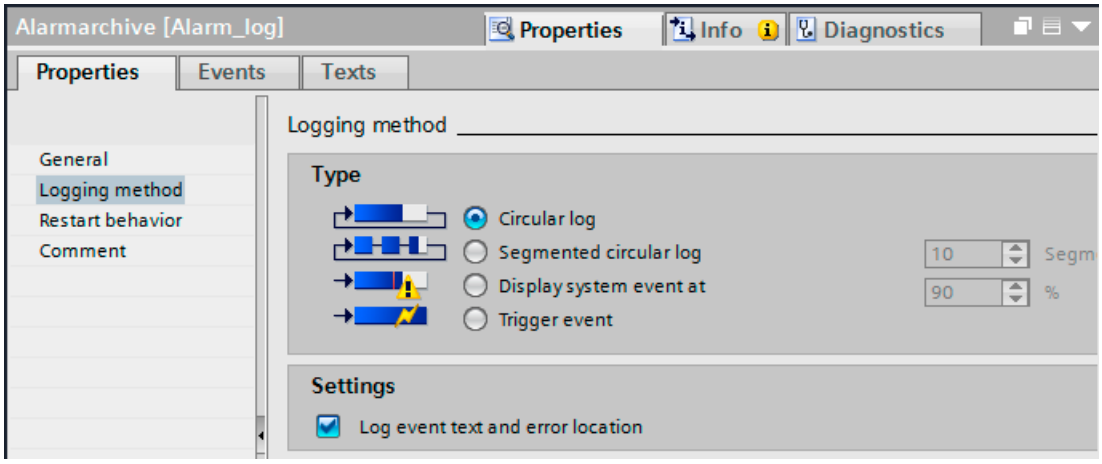
- WinCC reports
- SIMATIC Logon EventLog, on the computer with the SIMATIC Logon installation
- Event Viewer in the Windows Computer Management only for WinCC RT Advanced (logon/ logoff actions, account management, rights settings for the file system, etc., according to the corresponding configuration)

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

7.7.2 Recording and archiving

Tag and alarm logs are defined in the "Historical data" editor for continuous archiving of process-relevant data. The configured logging method determines the reaction if the log is full.

- Circular log
  The oldest entries are deleted.
- Segmented circular log
  The entries are stored in defined segments. When all segments are filled, the oldest segment is deleted.
- Display system event at a definable fill level
  A system alarm is triggered when the fill level is reached.
- Trigger event at full log



A checksum can be generated for each log entry for logging methods "Display system event at..." and "Trigger event" in combination with CSV and TXT formats. This enables any manipulation of the archives to be detected. The checksum is checked when the archives are opened in the Audit Viewer application, see chapter "Audit trail (Page 131)" - Viewing the audit trail.

The size of the archive depends on the length of a single entry and the number of entries. It is defined in number of entries. The size of the memory card must be taken into account here for HMI devices.

See also

- TIA Portal Information System > Visualize processes > Working with tags > Archive tags > Data logging (Basic Panels, Panels, Comfort Panels, RT Advanced) > Working with data logs (...)
- TIA Portal Information System > Visualize processes > Working with alarms > Alarm logging > Configuring alarm logging (Panels, Comfort Panels, RT Advanced)
- TIA Portal Information System > Visualize processes > Working with logs

The CSV, TXT and RDB formats are available as file formats. Archiving in RDB format, a proprietary database, provides fast access to data for displaying the data in the controls during runtime. For further evaluation of the data, the RDB format must be converted into the CSV format using the copy function. Archives in CSV / TXT format can be evaluated with other tools. The TXT format is Unicode-compliant and therefore suitable for Asian fonts.

Archiving language

The archiving language is specified in the general runtime settings of the HMI device. If a change of language is intended in the operator interface, it is recommended that one of the set up languages be specified as the archive language so that archiving always occurs in the same language.

Note

For panels, we recommend archiving of tags, alarms and audit trails locally on a memory card and cyclically transferring of the archives to a network drive.

See also

- Chapter "Connection to a network drive with access control (Page 140)"
- TIA Portal Information System > Visualize processes > Working with system functions and Runtime scripting > Reference > Function list > System functions (Basic Panels, Panels, Comfort Panels, RT Advanced) > Archive (...)
- Safely copy and move archives, Online Support under entry ID 63042926 (https://support.industry.siemens.com/cs/ww/en/view/63042926)

7.7.3 Archiving batch data with PM-QUALITY

The WinCC Premium Add-on PM-QUALITY offers batch-based archiving of process data and alarms, see also chapter "Archiving batch data with PM-QUALITY (Page 110)".

PM-QUALITY is installed on a separate computer or on the computer with WinCC RT Advanced. PM-QUALITY records the batch data from multiple, parallel operating production units in a separate database. A tag connection to panels or WinCC RT Advanced or directly to an S7 controller is established via OPC UA. Various ActiveX controls, for example, for viewing the batch data or trends, are available in WinCC RT Advanced for integration in a process screen. PM-QUALITY can be operated as a standalone system on a PC as an alternative. Applications for displaying and managing the batch data are included in the scope of delivery.

See also

- PM-QUALITY (http://www.siemens.com/pm-quality)
- Process Management (http://www.siemens.com/process-management)

7.7.4 Connection to a network drive with access control

To enable back up of the locally stored archives, the panel is connected to a network via the Ethernet interface.

See also

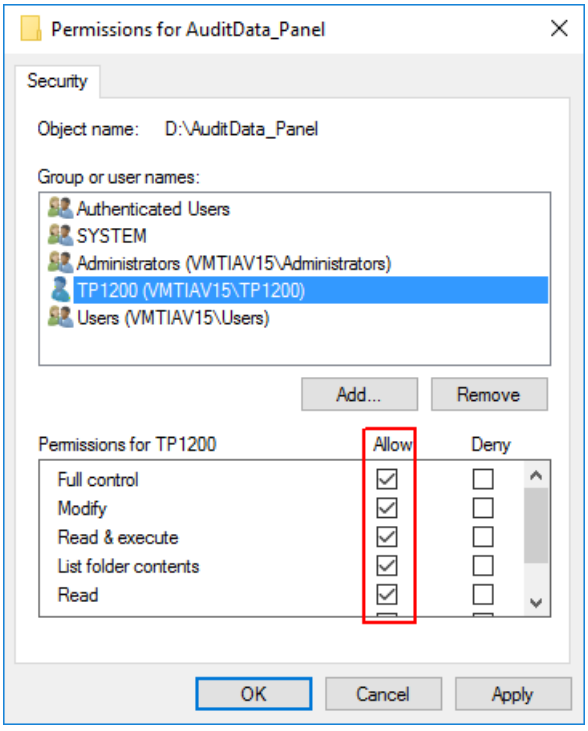
- Integrating an HMI operator panel in a local network, Online Support under entry ID 13336639 (https://support.industry.siemens.com/cs/ww/en/view/13336639)

Note

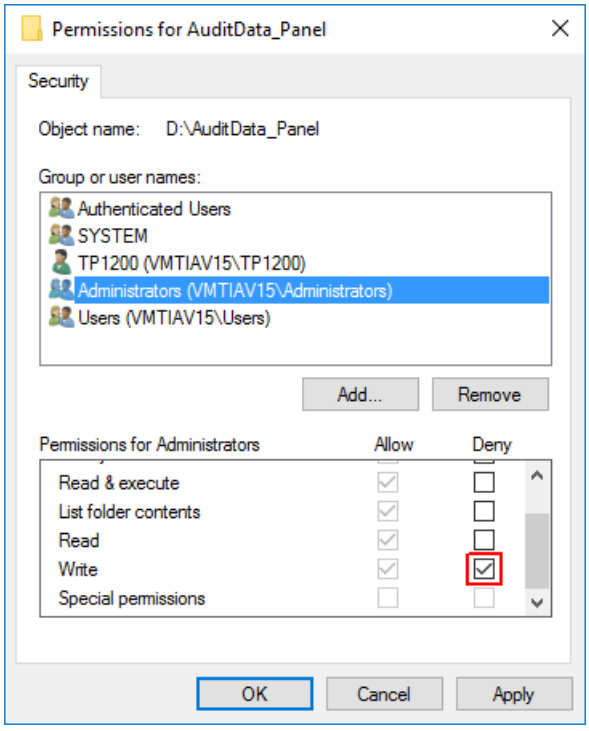
The folder in which the data is stored by the panel must be secured with Windows tools to protect the CSV and TXT files against unauthorized user manipulation.

The following procedure is recommended for this purpose:

- A new user is created with the name of the panel in the Windows user management of the PC to which the archive data is moved to the shared folder. The name of the panel was specified when the network connection was configured in the control panel under network. This is the name by which the panel logs on to the network.
- The access rights for the shared folder are defined in the folder properties in the "Security" tab. The panel name is added under "Group or user names" and is assigned "Full control" under permissions.



- For the user groups "Users" and "Administrators", the check box under "Deny" is selected for the write authorization ("Write").



The panel is authorized to store the archive files in the directory based on this configuration. All other users can only read the log files. However, consideration should be given to creating an HMI administrator who has write access to the directory in case of emergency.

Note

If the archive data is placed in a subfolder of the shared directory, then it is sufficient to make the security settings for this folder.

The screenshots were taken in the Windows 10 operating system.

7.8 Reporting

7.8.1 Output of process and production data

Process data can be output in report form on a network printer or stored in PDF / HMTL format.

The following data can be reported:

Tag contents	Current process values
Alarm report	Alarms from the alarm buffer or from the alarm log
Audit trail	Operator action entries

Tag contents	Current process values
Recipes	Data records of recipes in tabular form
Hardcopy	Hardcopy of screen content

The report layout can be designed with a title page, header and footer, multiple detail pages and a back page. For the display of process data, a series of objects and controls are available in the Tools area that can be moved to the report pages using drag-and-drop and then configured.

The scope of the data output can be specified as follows:

- Alarms: Output of the alarm buffer or the alarm log
  A time range from ... to can be specified.
- Recipes: Output of a particular recipe for each integrated control
  For this recipe, either all data records, a specific record or a range of data record numbers are printed.
- Audit trail: Output of the complete audit trail entries that were archived on the HMI device.
- Hardcopy: Printout of the current screen content using the "PrintScreen" system function

See also

- TIA Portal Information System > Visualize processes > Working with reports > Basics (...)

Activation of the printout

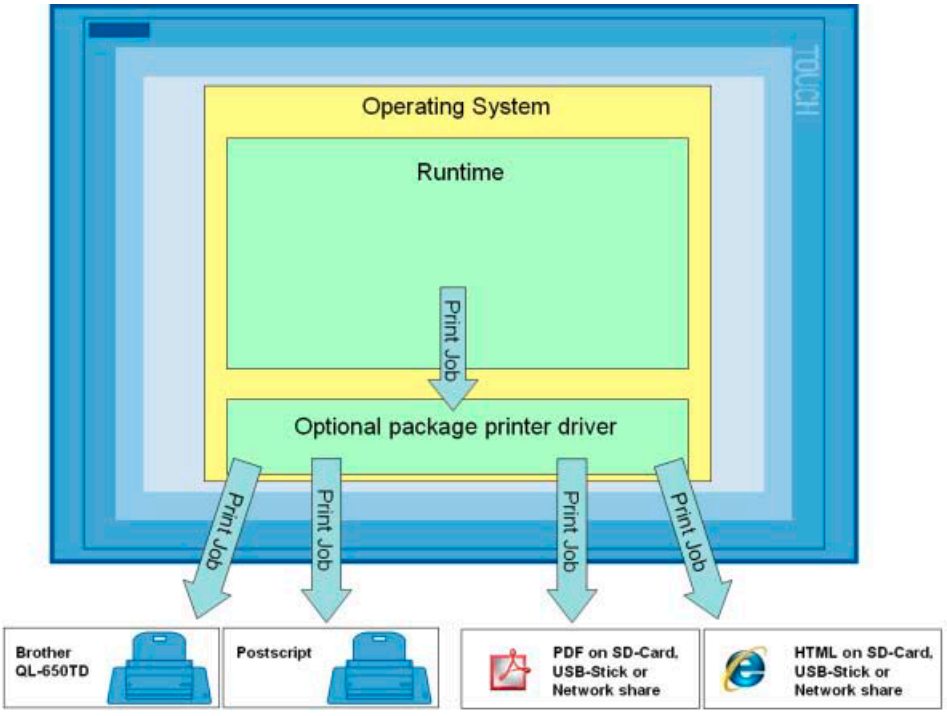
The output to the default printer is organized with the "PrintReport" system function. The system function can be launched either with a button or cyclically in the task scheduler.

Reporting on a network printer or another printing option

The following alternatives are available for printing reports:

- Network printer
- Postscript printing (printing with PostScript compatible printers)
- Brother QL-650TD (thermal printer)
- PDF printing (output in a PDF file)
- HTML printing (output in an HTML file)

Printer drivers for Comfort Panels are available in an options package for printing to PDF/HTML files and for the PostScript printing and Brother QL-650TD options. These drivers can be installed on the HMI device using the ProSave application. Reports in the PDF/HTML file format can also be stored on a USB stick or a network drive as an alternative to local storage on a memory card.



See also

- List of recommended printers, and printer driver optional package with installation instructions, Online Support under entry ID 11376409 (https://support.industry.siemens.com/cs/ww/en/view/11376409)
- TIA Portal Information System > Visualize processes > Performance features > General technical specifications > Recommended printers
- TIA Portal Information System > Visualize processes > Performance features > General technical specifications > Printing via print server
- Setting up a network printer, Online Support under entry ID 18720136 (https://support.industry.siemens.com/cs/ww/en/view/18720136)

7.8.2 Batch-based reporting with PM-QUALITY

The WinCC Premium Add-on PM-QUALITY offers convenient reporting of batch data. In contrast to the continuous data acquisition on the HMI devices, recording of the relevant batch data begins with the start of the batch and stops at the end of the batch. The recorded data is assigned directly to a batch name / number.

In a system configuration with panels and WinCC RT Advanced, batch data is recorded as follows in PM-QUALITY:

- Process values from panels or WinCC RT Advanced or directly from the S7 controller via OPC connection
- Transfer of alarm logs from the panel or WinCC RT Advanced

- Transfer of the audit trail from the panel or WinCC RT Advanced
- Transfer of data logs from the panel or WinCC RT Advanced

The process values are acquired cyclically or event-driven directly in PM-QUALITY. At the end of the batch, alarm logs and the audit trail are moved to a network drive or another drive on the PC and read in there by PM-QUALITY into its own database.

PM-QUALITY Report editor provides a wide range of design and evaluation options for the display of batch data in a report.

See also

- Chapter "Batch-based reporting with PM-QUALITY (Page 112)"
- Chapter "Archiving batch data with PM-QUALITY (Page 140)"
- Process Management System (http://www.siemens.com/process-management)

7.9 Remote control of HMI devices with the Sm@rtServer option

The use of the WinCC Sm@rtServer option in combination with the WinCC Audit option is permitted in environments subject to validation only under certain preconditions. In order for operator actions to be reliably assigned to the current log-on user, the remote control / remote maintenance must additionally be interlocked. For this purpose, the connection to the web server is established only with an operator request and is terminated again after the operator input ends.

The establishment and termination of the connection to the web server is controlled by means of a tag synchronization in the HTTP protocol. An authentication is set up for the connection of the web client with the web server. In this way, the following requirements can be met:

- Only one HMI device can be used for operator input, either the server or client. The current user is automatically logged off before a changeover. A seamless changeover is not possible.
- The current user is logged off automatically when the web client connects to the web server or the remote-control screen is exited due to a change of screens. The web server is additionally stopped.
- If a connection is lost, the current user is logged off automatically and the web server is stopped. After the connection is restored, another operator request must be issued.
- The web server is only an operation when remote control is active.
- Only the operation control for one web client is approved.

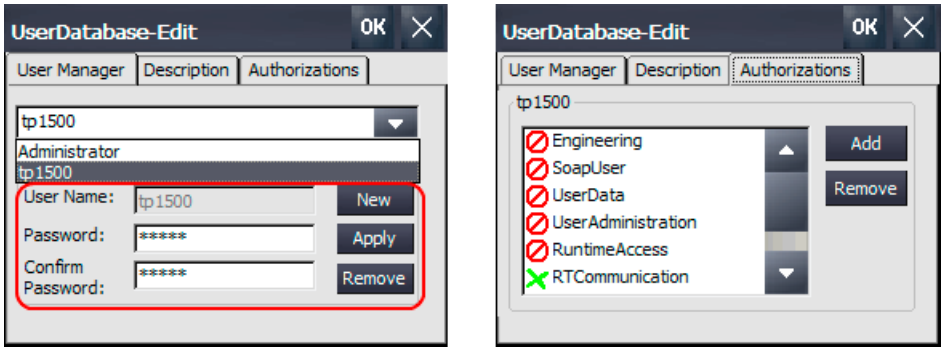
See also

- Remote control of operator panel in applications requiring validation in the pharmaceutical environment, Online Support under entry ID 49368600 (https://support.industry.siemens.com/cs/ww/en/view/49368600)

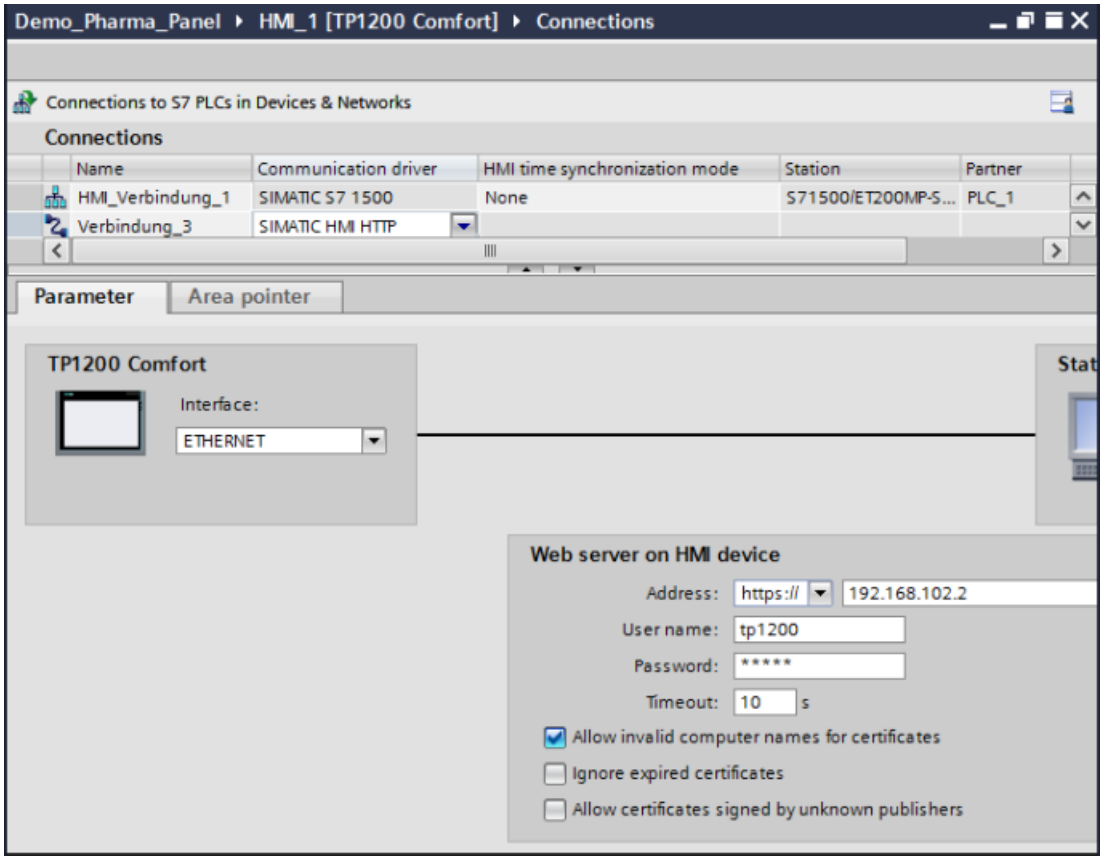
7.9.1 Secure HTTPS connection between HMI devices

A secure connection with certificate for exchanging tags between the web server and web client increases the security of the data exchange in the network. The certificate is generated on the web server at the first web client access. The certificate is transferred to the web clients and installed/imported there for each file transfer. Each time a connection is established, the web client checks whether the certificate is consistent with the web server.

As a further security measure, web users are created with password on the HMI device with the activated web server.



This user data is entered in the web client when there is a HTTPS connection.



During the certificate check, the time stamp and device name, among other things, are compared. For this reason, time synchronization of the HMI devices must be ensured. Because panels do not recognize the device name in the network, either the "Allow invalid computer names for certificates" property is activated or a domain or name server is configured in the network settings for the panel.

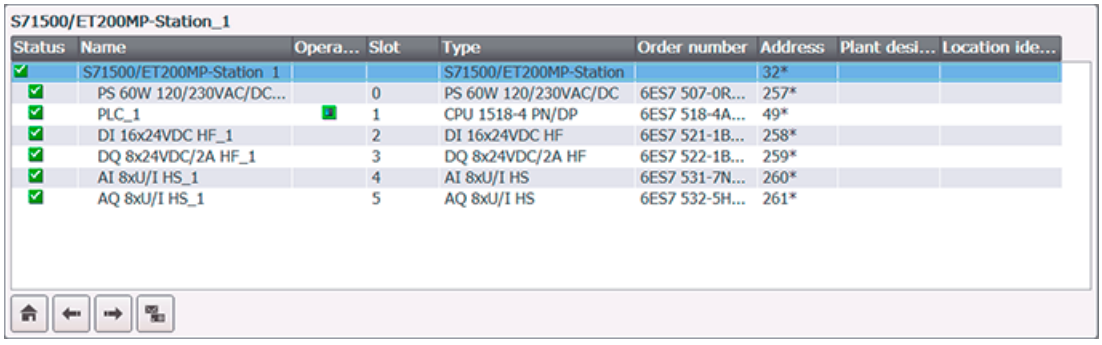
See also

- TIA Portal Information System > Visualize processes > Options > WinCC Sm@rtServer (Panels, RT Advanced) > Access via SIMATIC HMI HTTP Protocol (…) > Commissioning an HTTPS connection (…)

7.10 Monitoring of the system

7.10.1 Diagnostics of the communication connection

The status of the connection to lower-level controllers can be visualized with the "System diagnostics view" control. The device view shows the available devices of a level in a table (see figure). Information on the status and error entries are displayed in the detail view, which can be opened by double-clicking the device in the table.



The control can be integrated, for example, in a diagnostic screen.

See also

- TIA Portal Information System > Visualize processes > Creating screens > Display and Control Objects > Objects

7.11 SIMATIC HMI Option+

The SIMATIC HMI Option + application provides information about the hardware of a Comfort Panel. The application acts as a gateway between the runtime and the operating system and also enables the configuration of IT-related functions. It is loaded and configured on the HMI device via the ProSafe tool. Access for the configuration is only approved to authorized personnel and is password protected.

The evaluation and display of the respective data are explicitly selected in the configuration. The application provides the results of the evaluations in predefined tags that can be integrated, e.g. in a separate service screen, for display in the runtime project.

The application returns the following information:

- Panel data such as type, version, order number, TIA Portal version
- Runtimes since the last runtime start / since the last firmware update
- Resources of the available memory (Flash, SD card)
- Display of active client connections with IP address or host name
- Acceptance and take over of certificates for OPC UA and / or SIMATIC Logon Remote Access connections, for example
- Support of the PM-LOGON Basic option for logging on via a card reader
- Faceplate for controlled connection or disconnection of USB storage media
- Hiding the desktop icons when booting the panel, for example.

In conjunction with the option Sm@rtService, the service screen with the information can also be called up via remote access.

See also

- The plus for more options - SIMATIC HMI Option + (https://w3.siemens.com/mcms/human-machine-interface/en/operator-devices/advanced-hmi-panel-based/Pages/hmi-option-plus.aspx)

7.12 Interfaces

7.12.1 Connection of SIMATIC S7

Comfort Panels and PC systems with WinCC RT Advanced are equipped with communication drivers, for example, for SIMATIC S7-1200, SIMATIC S7-1500, and SIMATIC S7-300/400. A connection is established via MPI / PROFIBUS DP or Ethernet. The physical connection and logical connection are configured in the "Devices & networks" editor.

The tag management is the data interface between the S7 and the HMI device. All editors integrated in WinCC read and write data in tag management. Through the integration in the TIA Portal engineering interface, there is direct access to the PLC tags (external process tags) and the HMI tags (internal tags of the HMI device) in the editors for configuring the HMI device. Changes to S7 data that are used in the HMI device (for example, PLC tags, data block assignment) are automatically updated in the projects of the connected HMI devices when the project data is compiled.

An interruption of the communication connection is automatically indicated with a system alarm in the HMI alarms. The connection status can be visualized in a process screen with the "System diagnostics view" control.

See also

- TIA Portal Information System > Visualize processes > Communicating with PLCs > Device dependency > Comfort Panel / PC systems with WinCC Runtime
- Chapter "Diagnostics of the communication connection (Page 147)"
- Chapter "Inter Project Engineering (IPE) (Page 72)"

Password for connection establishment

The data connection between the HMI device and the S7-1500 automation system can be password-protected with the "HMI access" protection level. The password is defined in the CPU.

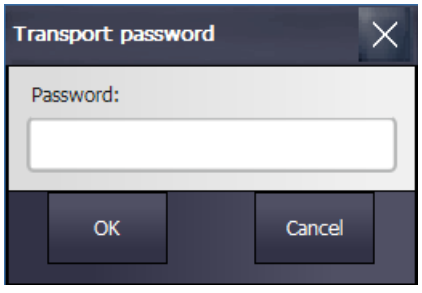
The same password must also be specified in the project data of the HMI device when connecting to the CPU. Together with the project data, this is downloaded in encrypted form to the HMI device. A connection between the HMI device and PLC is only established if the configured passwords in both devices match.

See also

- Chapter "Protection functions in the automation system (Page 160)"

Transport password

The transport password protects the transfer of project data to the target system. The configured password is queried once when the data is transferred to the runtime system. If the password was specified correctly, the certificate is stored in the certificate memory and the project data is transferred to the HMI device.



See also

- TIA Portal Information System > Visualize Processes> Compile and Download> Runtime Advanced and Panels> Settings for Runtime> Password Protection in Runtime (...)

7.12.2 Connection to other components and third-party suppliers

The HMI devices have an OPC interface for connecting to other components as well as third-party suppliers. An HMI device can be used as an OPC server and/or OPC client. The type of the OPC connection depends on the device. Comfort Panels communicate via a secure OPC UA connection. For systems with RT Advanced, the older OPC DA interface is also available in addition to the new OPC UA technology.

See also

- TIA Portal Information System > Visualize processes > Interfaces > OPC > OPC for Runtime Advanced (Panels, Comfort Panels, RT Advanced) > Basics (...) > Using OPC in WinCC (...)

7.12.3 Connection to SIMATIC WinCC RT Professional

HMI devices with WinCC RT Professional and with WinCC RT Advanced and Comfort Panels might be implemented in a distributed system.

Tag contents are exchanged via the OPC interface.

See also

- Chapter "Connection to other components and third-party suppliers (Page 126)"

Central audit trail

Audit trails that are generated by the individual HMI devices as a circular log in CSV format can be imported into the database of the alarm system of WinCC RT Professional with the PM-OPEN IMPORT add-on. A distinction is made between operator input alarms, alarms and system alarms.

In the case of operator input alarms, it must be noted that they are assigned the number of the standard operator input alarm in WinCC RT Professional (12508141). Old value and new value are also transferred to the process value blocks 2 and 3. The original time stamp of the alarms is preserved when importing data.

The import of data is organized as follows:

- Installation of the PM-OPEN IMPORT add-on on the PC with WinCC RT Professional
- Creating a Windows directory for each HMI device into which the CSV files are moved either event-driven or cyclically

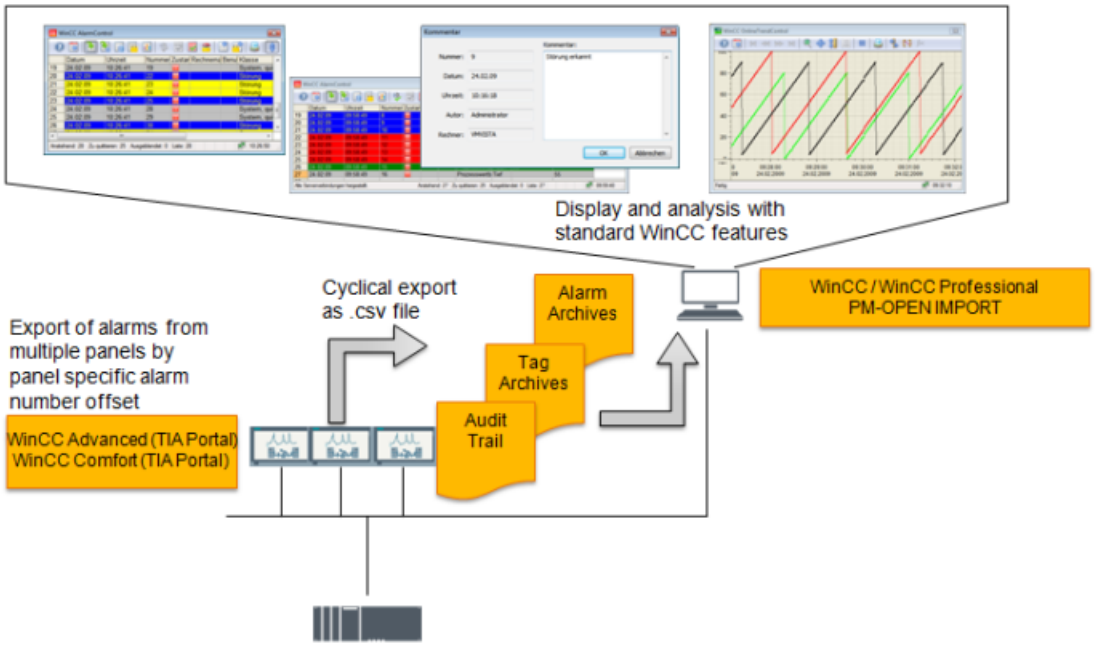
The directories are monitored by PM-OPEN IMPORT with Windows tools. As soon as a CSV file is detected in the directory, PM-OPEN IMPORT starts reading in the data.

The imported audit trail entries can be displayed in a process screen by WinCC RT Professional with the ActiveX Control "Alarm view".

Central process value archiving and central alarm management

Data and alarm logs that are generated by the individual HMI devices as a circular log in CSV format can also be transferred to the databases of WinCC RT Professional with the PM-OPEN IMPORT add-on. Data from the data log are read into the data log of WinCC RT Professional and alarms into the alarm log. The original time stamp remains unchanged. Logging tags and alarms must be created beforehand in WinCC RT Professional. In order to differentiate the alarms, an offset is configured for the alarm number for each HMI device.

The imported data can be displayed in WinCC RT Professional using the trend / table view or the alarm view.



Configuration for SIMATIC S7-1500 Automation Systems

8

The automation task is described in the User Requirement Specification (URS), Functional Specification (FS) and Design Specification (DS). Besides the description of the functional sequence, the specifications describe the operation philosophy in manual/automatic/local modes and an alarm and security concept.

The hardware is planned and the user-specific software is prepared based on this documentation.

8.1 Creation of the user program

The user program includes both the hardware configuration of the automation system and the program code for the functional operation.

8.1.1 Hardware planning

The complete configuration of the automation system including all modules, connections, connection parameters and module properties is configured in the "Devices & networks" editor and downloaded to the PLC. Convenient diagnostic functions display faults in the TIA Portal engineering system or directly on the local display.

See also

- Chapter "Diagnostics in the TIA Portal engineering system (Page 174)"

8.1.2 Automation program

Before the start of programming, the automation task should be subdivided into smaller functional areas based on technological implications. Individual units such as valves, motors, pumps etc., are functionally identified and described. Functions that are repeated in the functional sequence, such as the control of valves or motors, are programmed, tested and validated in separate blocks. The program structure maps the required functional sequence, whereby the previously validated blocks are called up as required and only parameters still have to be assigned.

See also

- Chapter "Software categorization according to GAMP Guide (Page 185)"
- TIA Portal Information System > Programming a PLC > Programming basics > Blocks in the user program > Linear and structured programming

- Programming Guideline for S7-1200/S7-1500, Online Support under entry ID 90885040 (https://support.industry.siemens.com/cs/ww/en/view/90885040)
- "STEP 7 and WinCC Engineering" system manual, chapter 12 "Programming the PLC", Online Support under entry ID 109755202 (https://support.industry.siemens.com/cs/ww/en/view/109755202)

Software interlock / safety

The system must guarantee safe operation of the plant in all situations. In addition to taking this into consideration in the functional specification, appropriate measures taken during programming also contribute to the prevention of dangerous situations and to safety. Examples of this include:

- Incorrect inputs on HMI devices must not trigger incorrect reactions.
- Realization of Emergency Stop functions with fail-safe automation hardware or with suitable hardware devices.
- Controlling of output values of the analog output signals when the automation system switches to STOP state.
- Outputs to the process should only be controlled at one point in the program.
- Besides the cyclic processing, routines should be provided for starting and restarting the program after power failure as well as error handling and alarms.
- Diagnostic alarms for runtime, end position and limit value monitoring must be integrated in the blocks. These should be displayed on the connected HMI devices.

Programming languages

The CPU SIMATIC S7-1500 provides an innovative architecture for storing program data and thus also provides an increase in the program performance. The entry "Programming guideline for S7-1200/1500" presents the new programming options and a comparison with the previous PLC systems, see Online Support under entry ID 81318674 (https://support.industry.siemens.com/cs/ww/en/view/81318674).

See also

- TIA Portal Information System > Programming a PLC > Recommendations for programming

The TIA Portal supports the creation of error-free program code with convenient functions.

The following programming languages are available:

- LAD – Ladder Diagram (graphical, based on circuit diagrams)
- FBD – Function Block Diagram (graphical, based on electronic circuits)
- STL – Statement List

- SCL – Structured Control Language, a high-level Pascal-based script language based on IEC 61131-3.
  IEC 61131 (also EN 61131) addresses the basics of programmable logic controllers. Part 3 of the standard defines the programming languages.
- GRAPH – Graphical programming language for creating sequential control systems (CPU-dependent)

The programming language can be specified for each block. Graphical programming languages quickly communicate an overview of the programmed function. System-tested instructions matched to the selected programming language are provided, which also map system blocks depending on the complexity. The auto-complete function offers only compatible instructions and tags. Incorrect code entry is minimized by the syntax check. At the conclusion of code creation, the blocks are compiled and checked for the following aspects:

- General syntax check of the entire program
- Check of block calls for errors at the interfaces
- Unique block numbers
- Consistency of the program based on the time stamps that are assigned internally in the system when the individual blocks are changed.

See also

- TIA Portal Information System > Programming a PLC > Creating a user program > Compiling and downloading PLC programs

A separate check to see if the program has been run according to the recommendations in the "Programming Guide and Programming Styleguide for S7-1200 and S7-1500" can be performed using the Programming Styleguide Checker tool.

- Tool for checking STEP 7 (TIA Portal) program code with the "Programming Styleguide Checker", Online Support under entry ID 109741418 (https://support.industry.siemens.com/cs/ww/en/view/109741418)
- Programming Guideline and Programming Styleguide for S7-1200/1500, Online Support under entry ID 81318674 (https://support.industry.siemens.com/cs/ww/en/view/81318674)

Instructions

The instructions are categorized into

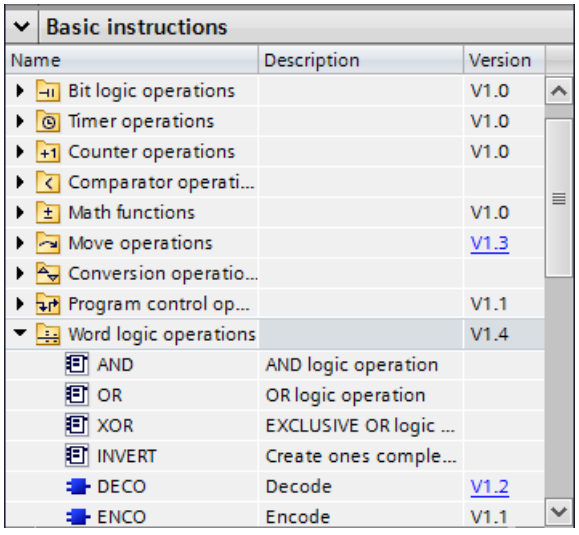
- Basic instructions
- Extended instructions
- Technology
- Communication

and are managed in the system library.

Note

When the individual blocks are created, a check should be made to determine to what extent functionality can be covered by the instructions offered on the product side. An instruction is already system-tested by default and reduces the amount of the validation effort associated with category 5 user-specific software (see chapter "Verification of software (Page 184)"). Only parameters still have to be assigned for the call-up.

An instruction for a complex function maps a system block. The system library is also updated when the engineering system is upgraded. Changes to individual instructions are marked by a version number. If the major version is incremented, this signifies a more significant change, possibly even to the interface. The minor version (position after the decimal) is incremented in the course of an error correction or minor changes. The same version of an instruction must be used within the user program. This is controlled automatically when the program is compiled.



See also

- TIA Portal Information System > Programming a PLC > Program editor > Using instruction versions
- Comparison list for programming languages, Online Support under entry ID 86630375 (https://support.industry.siemens.com/cs/ww/en/view/86630375)
- Library with general functions (LGF) for STEP 7 (TIA Portal) and S7-1200 / S7-1500, Online Support under entry ID 109479728 (https://support.industry.siemens.com/cs/ww/en/view/109479728)
- Example blocks for STEP 7 (TIA Portal) and WinCC (TIA Portal), Online Support under entry ID 66839614 (https://support.industry.siemens.com/cs/ww/en/view/66839614)
- Program examples from the TIA Portal Information System, Online Support under entry ID 109476781 (https://support.industry.siemens.com/cs/ww/en/view/109476781)

Program flow control

Runtime errors during program execution cause the program to abort. To prevent this, some functions in the LAD/FBD programming languages have the EN/ENO mechanism. Instructions are executed if the EN enable input has the signal state "1". After error-free execution of the instruction, the ENO enable output also has the signal state "1". The error case with signal state "0" can be evaluated by the calling block.

In the STL, SCL and S7-GRAPH programming languages, a status word can be evaluated correspondingly.

See also

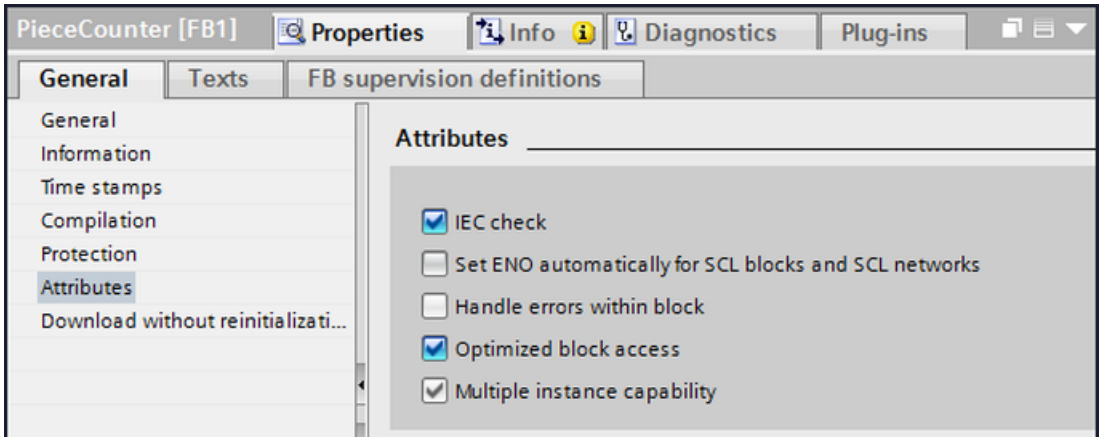
- TIA Portal Information System > Programming a PLC > Programming basics > Program flow control
- TIA Portal Information System > Programming a PLC > Programming basics > Handling program runtime errors > EN / ENO mechanism

Implicit data type conversion

An implicit data type conversion is always performed where data of different types is jointly processed, for example, in comparison operations or arithmetic operations.

To prevent inaccurate values resulting from the data conversion, the stringent check according to IEC 61131 can be activated for blocks. Incompatible operands must then be converted explicitly by appropriate software instructions.

The IEC check property can be activated as the default setting for all new blocks or set separately for each block.



Detailed information regarding implicit and explicit conversion of the individual formats is documented in the TIA Portal Information System > Programming a PLC > Data types > Data type conversion for S7-1500.

See also

- TIA Portal Information system > Programming the PLC> Data types > Data type conversions for S7-1500> Implicit conversions (S7-1500)> Activating or deactivating the IEC check
- Programming Guideline and Programming Styleguide for S7-1200/1500, Online Support under entry ID 81318674 (https://support.industry.siemens.com/cs/ww/en/view/81318674)

Optimized block access

New blocks are created with the "Optimized block access" property by default in the SIMATIC S7-1500. In contrast to the SIMATIC S7-300/400 automation systems, the tag declarations are implemented universally with symbolic names of the data elements. As a result of this, the absolute addresses can be managed and optimized automatically by the system. This increases the program performance and minimizes errors.

The "Optimized block access" property can be deactivated/activated for each block. After a migration of STEP 7 projects for the S7-300/400 automation systems to S7-1500, the "Optimized block access" is deactivated by default. If the requirements indicated in the documentation are met, this property can be activated subsequently for each individual block.

See also

- TIA Portal Information System > Programming a PLC > Programming basics > Blocks in the user program > Blocks with optimized access

Retentive tag declaration

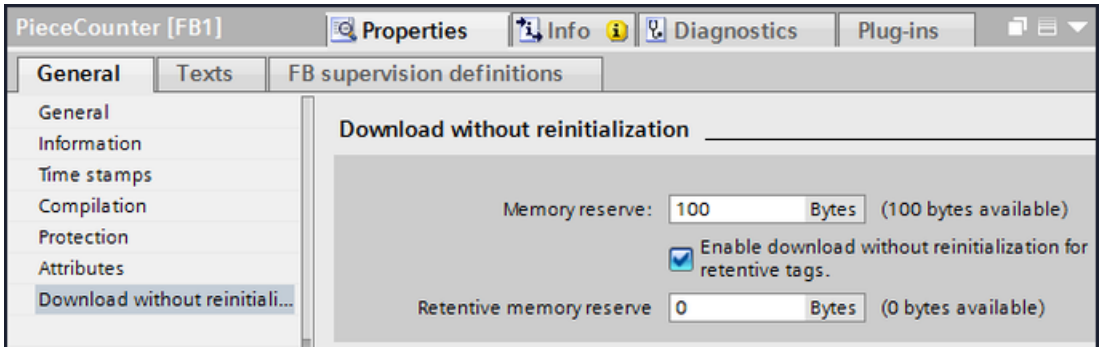
To prevent data loss in the event of power failure, the "Retentive" property is activated for data blocks. As a result, this data is stored in retentive memory.

Instance data blocks always have the same block access (standard for optimized) as the associated function block. In the case of optimized block access, the "Retentive" property can be activated not only for the complete data block as with S7-300/400 but also for individual data elements in the data block or for individual tags at the interface of the function block. The "Retention" property is available for individual tags for global data blocks with optimized block access as well.

Extending the block interface

A memory reserve of 100 bytes is set for each function block in the SIMATIC S7-1500 by default (configurable). Additional retentive memory area can be defined.

This memory reserve is used if the block is to be extended subsequently at its interface during operation of the user program. The "Download without reinitialization" property prevents overwriting of the tags marked as retentive.



The assigned retentive memory area can be canceled again at a later time, for example, when the plant is shut down. It must then be taken into consideration when starting the plant that the initial values and not the retentive values are activated. The release to memory area can be used again for extensions.

Note

Each change during the operational phase must be agreed on with the process owner and documented and implemented according to the change control procedure. In the case of a complete reinitialization, the corresponding effects must be noted.

See also

- TIA Portal Information System > Program a PLC > Compile and download PLC programs > Download blocks (S7-1200, S7-1500) > Download block extensions without reinitialization (…) > Reset the memory reserve (…)
- Programming Guideline and Programming Styleguide for S7-1200/1500, Online Support under entry ID 81318674 (https://support.industry.siemens.com/cs/ww/en/view/81318674)

Supporting functions during programming

In order to create consistent and error free software, the TIA Portal offers many types of program information in the PLC programming area.

- **Cross-references** provide an overview of all used operands, blocks, tags, and screens, each with point of use (including jump), relation to one another and type of use. Filters for source and reference objects as well as user-defined filters support program testing or troubleshooting.
- **Assignment list** provides an overview of the assigned operands within the program.
- **Call structure** represents the call hierarchy of the blocks and provides an overview of the use of the blocks.
- **Dependency structure** shows a list of utilized blocks with instance data blocks and their dependency on other blocks.
- **Resources** shows the hardware resources of the CPU for objects (such as OB, FC, FB, DB), for CPU memory areas and for the I/O modules.

See also

- TIA Portal Information System > Program a PLC > Show cross-references
- TIA Portal Information System > Programming a PLC > Displaying program information

8.2 Protection functions in the automation system

The automation systems (S7-300/400 and S7-1500) are equipped with protection functions for preventing unwanted access to program data over the network. The SIMATIC S7-1500 provides an additional protection level for a controlled network connection to HMI devices. Local unauthorized interventions are prevented by the display protection on the device.

All the indicated automation systems have know-how protection for safeguarding the block contents.

The protection functions for the SIMATIC S7-1500 are explained in the following.

8.2.1 Protection levels

For access to the program data of the PLC with a TIA Portal engineering system or an HMI device, protection levels, graded by operation level, can be set up. Each protection level can be provided with a password. The configured settings take effect after downloading to the automation system.

The effect of the various levels of protection is described in detail in the TIA Portal Information System, see the reference at the end of the chapter.

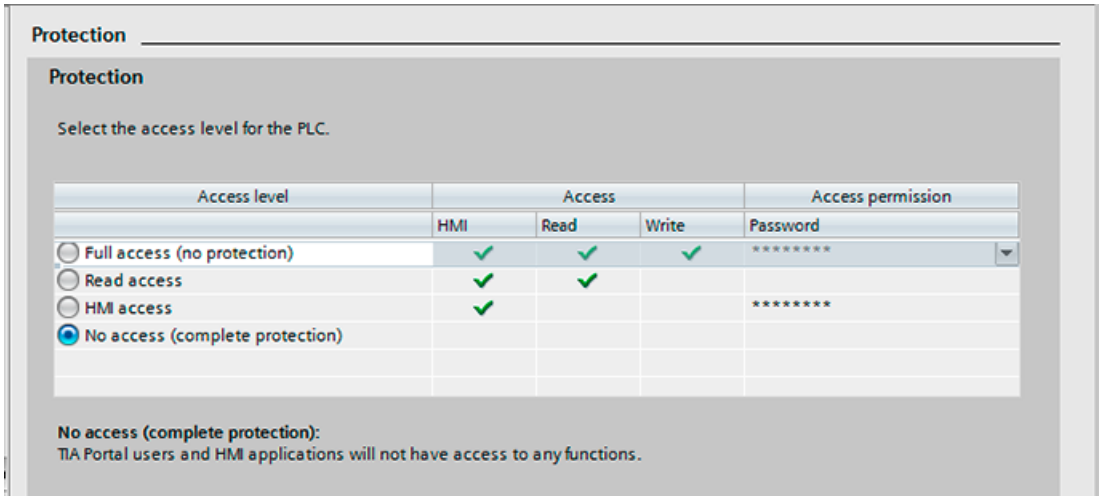
The entry of the password for read-only or read/write access is requested the first time an online connection is established with the automation system. Access authorization is in effect for the duration of the online connection or until the access authorization is manually canceled via the menu item Online> Delete access rights.

Password-protected functions can only be executed from an engineering system. It is not possible to log onto the PLC in parallel.

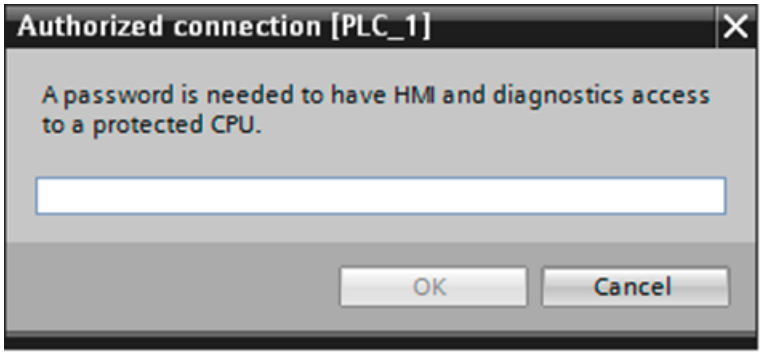
An additional protection against full access with password during RUN mode can be configured locally on the CPU display. Full access is only enabled when the hardware switch on the CPU is in STOP position.

"No access (complete protection)" protection level:

When complete protection is activated, a password must be entered for full access. In addition, a separate password can be specified for the "Read access" and "HMI access" protection levels, respectively. If the password has not been specified there, the password for full access applies.



To start the download operation to the PLC, the password for full access must be entered in the "Load preview" dialog. The password is also required for forcing/modifying tags, changing the operating mode online, etc.



Note

It is strongly recommended that the "No access" protection level be configured at the latest for the commissioning. If the PLC access is not protected, data can be downloaded from any TIA Portal engineering system using the "Accessible devices" function and connect online (see chapter "Backup of the automation software (Page 194)").

So that the connection between the HMI device and the SIMATIC S7-1500 can be established successfully, the password for HMI access must be specified in the HMI project data under Connections. This is either a separate password or the password for full access. The project data is downloaded to the HMI device. When the tag connection between the HMI device and PLC is established, the HMI password for the connection is checked. The connection is only established when there is a match.

"HMI access" protection level:

When this protection level is configured, a tag connection from the HMI device to the SIMATIC S7-1500 is allowed without entry of a password. The reading of diagnostic data is also allowed. All other actions require a password for write access (full access), optional for read access.

"Read access" protection level:

The setting of this protection level provides users read access to the data. For example, online information and diagnostic data can be called. A password must be configured for full access.

"Full access (no protection)" protection level:

When this level is activated, the CPU program is not protected. The user is given full access to all functions. The setting is not recommended.

"Full access including fail-safe (no protection)" protection level:

Fail-safe CPUs have an additional protection level that must be provided with a password for full access to the program data, including the fail-safe functions.

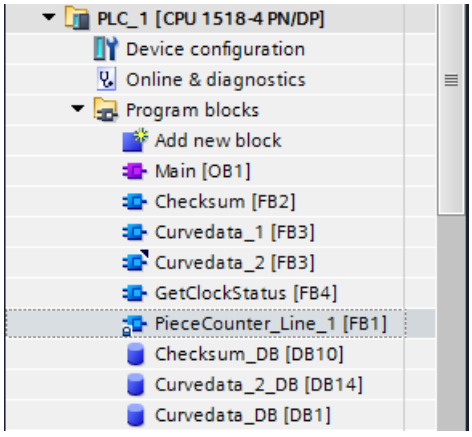
See also

- TIA Portal Information System > Communicating with controllers > Communicating with SIMATIC S7-1500 software controller> Communication via PROFINET parameters (communication via PROFIBUS parameters) > Protection of communication

8.2.2 Know-how protection for blocks

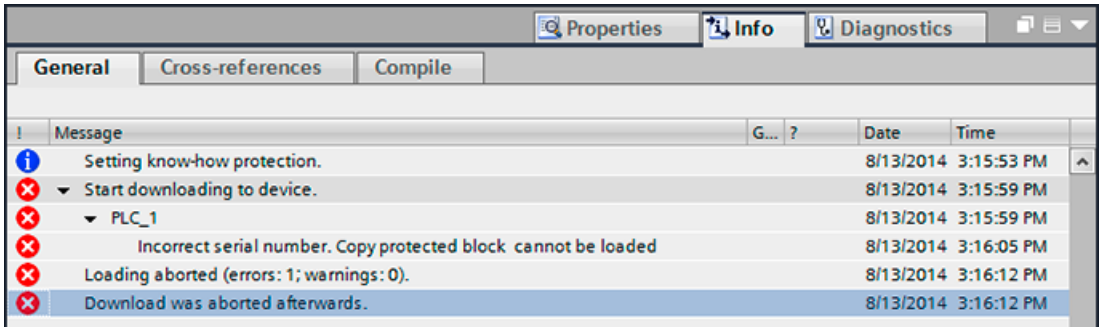
For protection of the block content, know-how protection can be set up for the following block types: organization blocks (OB), function blocks (FB), functions (FC) and global data blocks. This is configured separately for each block in the form of a password. Without the password, it is possible to read the block title, block parameters, call structure of the program and global tags. In addition, the blocks can be copied, deleted and integrated in the program. The block content is displayed only after the corresponding password is entered. Changing the block is only possible if the password is known.

A protected block is marked with a lock in the project tree.



Copy protection

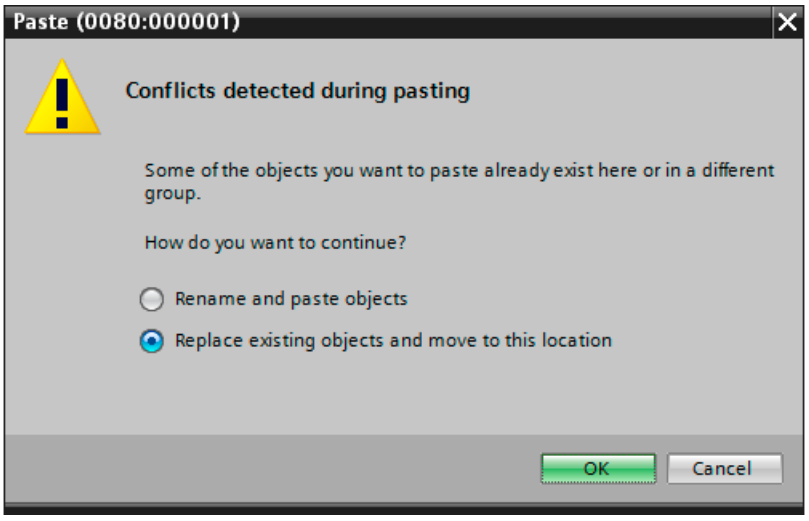
In addition to know-how protection, copy protection can be activated. The copy protection acts in combination with a serial number either from the memory card or the CPU. This is specified when copy protection is activated in the engineering system. When the software is downloaded to the PLC, a check is made to determine whether the configured serial number matches that of the connected device. As soon as an error is identified for a block, the complete download operation is canceled even if the block is not being called in the software.



Protected blocks in the library

A protected block can be stored in the project library or in a global library as a master copy. In so doing, the password is also transferred with the block data. Protected blocks are not specially marked in the icon in the library, however.

When the block is inserted from the library into the program, a conflict may occur if the block name already exists in the program. In this case, a dialog for selecting the corresponding action is displayed.



If "Rename and paste objects" is selected, the name is changed automatically and the block is inserted in the project tree. In order to change the block number, it is necessary to enter the password for know-how protection.

Note

The password is also retained if the block is stored in the project library or a global library.

See also

- TIA Portal Information System > Programming a PLC > Creating a user program > Protecting blocks

Connection to an external password provider

The TIA Portal provides an interface for connecting to an external password provider, which provides passwords for copy and write protection of the blocks. When assigning to a block, only the password names and not the passwords are displayed in a list. When a block is opened, the TIA Portal automatically connects to the password provider and retrieves the corresponding password. As the passwords are usually not known, the blocks remain protected even if the team of users changes.

If the password provider is not reachable, the manual input of the passwords can be permitted in a fallback strategy.

See also

- TIA Portal Information System > Programming a PLC > Protecting blocks > Connect password provider

8.2.3 Local display protection

Operator inputs on the display of the SIMATIC S7-1500 can be password-protected. This password is specified in the properties of the SIMATIC S7-1500 and downloaded with the hardware configuration to the CPU. The display protection can then be activated and deactivated on the display using Settings > Lock / Unlock. As soon as protection is activated, entry of the display password is required for any configuration change. However, alarms and diagnostic information can be called at any time without entering the password.

Extended protection

Protection in addition to the configured protection levels for the program data (local lock) can be set for the display of the SIMATIC S7-1500 under Settings > Protection. This protection is active while the mode switch (hardware switch) is in RUN position.

The protection is divided into three levels:

- Password for full access
- Password for read access
- Password for HMI access

For each level, "Allow" or "Deactivate in RUN" can be selected. In the Deactivate in RUN setting, the protected functions cannot be executed in RUN mode even if the required password is known. For example, downloading of program changes with password is only possible when the mode selector (hardware switch) is in the STOP position.

See also

- TIA Portal Information System > Editing devices and networks > Configuring devices and networks > Creating configurations > Automation systems (S7-300, S7-400, S7-1500) > Method of operation of S7-1500 CPUs (S7-1500) > Disable online access to CPU via display (…)

Hardware protection

The display can also be mechanically removed during RUN mode. When this happens, the underlying memory card and the RUN/STOP mode switch are freely accessible. When the memory card is removed, the CPU switches to STOP state. For this reason, unauthorized removal of the display must be prevented. For example, the display can be securely connected to the enclosure with a seal or lock by means of an existing eye. Otherwise, local access to the automation hardware should be appropriately safeguarded.

8.3 Recipes and data logs

8.3.1 Recipes

The SIMATIC S7-1500 offers the ability to manage simple recipe or parameter data records. Change control for these recipe data records is not available, however.

Note

Due to the lack of change control, this function must not be used in GMP-relevant plants.

8.3.2 Data logs

Current values from the CPU can be written in data logs. These are files in CSV format that are created on the SIMATIC memory card in the data logs directory or in the internal load memory. There is no concept for archiving of these data logs. The CSV format is not protected from data manipulation.

Note

For lack of the possibility to archive data, this function should not be used for GMP-relevant uses.

8.4 Web server of the CPU

The SIMATIC S7-1500 has a web server that can be activated in the CPU properties, if required. Diagnostic information, operating mode, device information and device status as well as tag status and watch tables can be called with a browser via the network. Additional functions are, for example, the listing of files and directories on the SIMATIC memory card via a file browser and online backup of the CPU configuration. All functions for web access are approved in the CPU properties and are protected with web username and password.

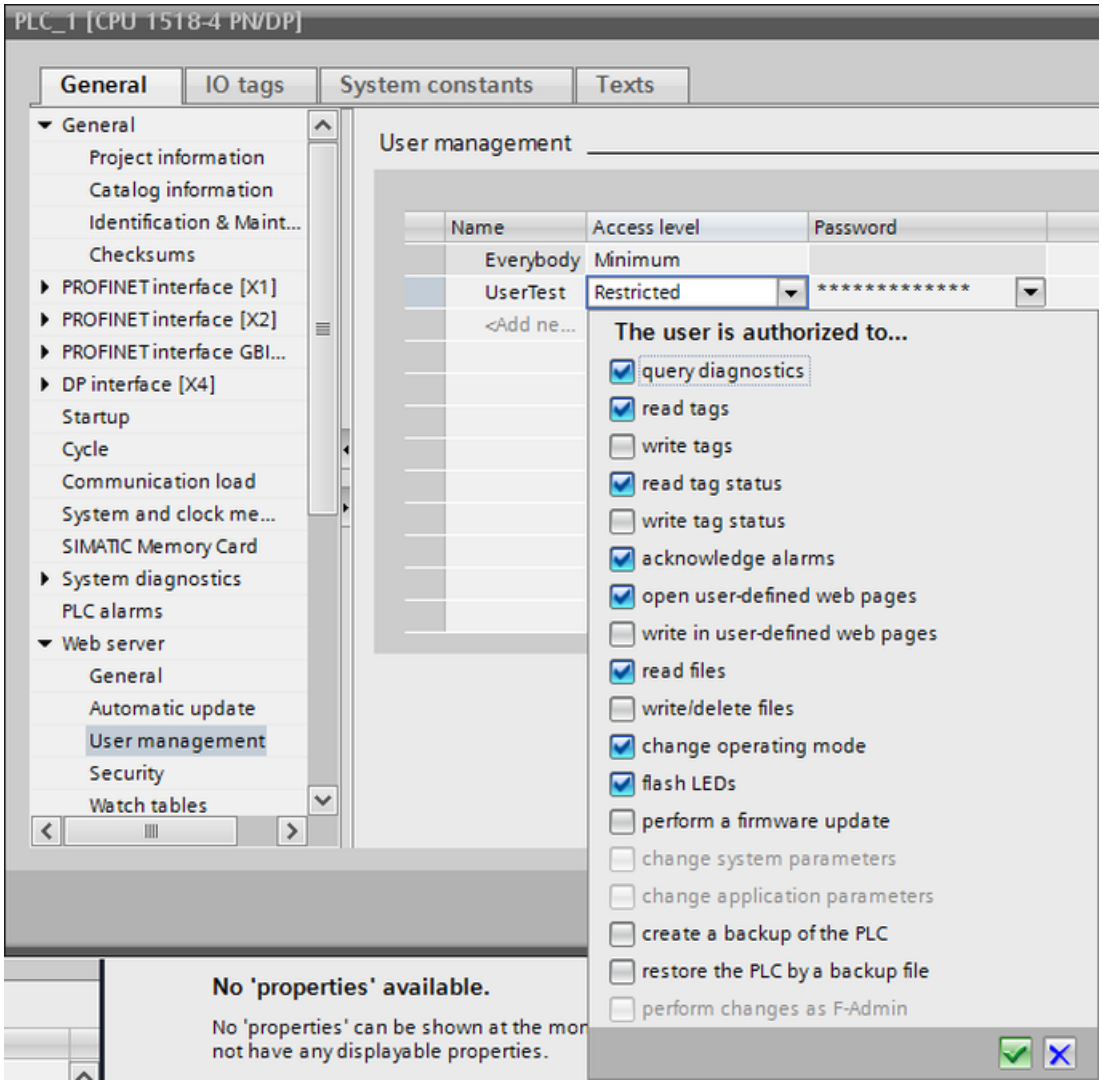
With HMI devices and mobile devices, web access is possible in a reduced display.

See also

- TIA Portal Information System > Editing devices and networks > Configuring devices and networks > Creating configurations > Configuring automation systems (S7-300, S7-400, S7-1500) > Configuring a web server (…)
- Chapter "Data and information security (Page 64)"

8.4.1 User Administration Web Server

Users that log onto the web server interface are configured with a password in a separate user administration. The operator input in the web server is dependent on the access levels that are approved for the logged-on user.



For establishing the connection, the IP address of the CPU is entered in the URL of the browser. If the IP address of the CPU is known, a connection to the web server can be established from each computer in the same subnet. Each connection to a browser is recorded in the diagnostic buffer of the CPU with IP address and session ID.

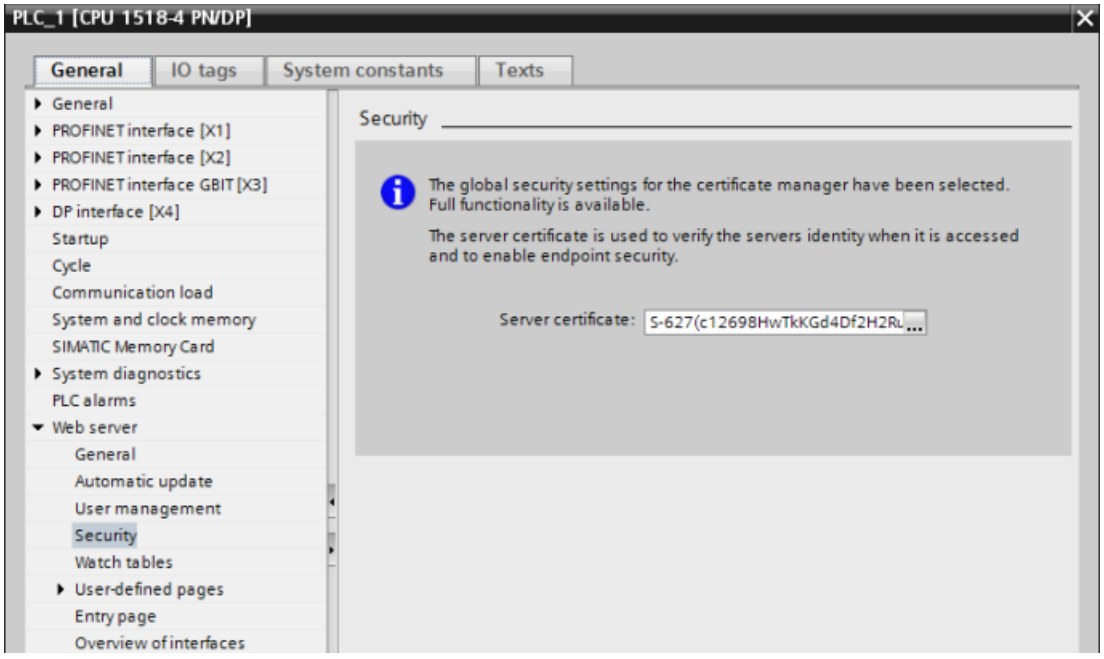
See also

- Chapter "Diagnostics in the TIA Portal engineering system (Page 174)"

In parallel to the connections between browser and web server of the CPU, an online connection for the TIA Portal engineering system to the STEP 7 program via a PG/PC can be active.

Note

It is recommended that access via external firewalls be limited appropriately or that a secure connection via HTTPS be established, see chapter "Secure communication (Page 170)".



See also

- TIA Portal Information System > Editing devices and networks > Configuring devices and networks > Creating configurations > Configuring automation systems (S7-300, S7-400, S7-1500) > Configuring a web server (…) > Standard websites (…) > Access only via HTTPS (…)

8.4.2 The web interface

The UserTest user is logged on to the web page. Depending on the enabled access rights, the user can make operator inputs, such as changing the operating mode. Menu items and buttons for which the user has not been granted access rights are not displayed.

Examples of functions provided via the web server interface include:

- Switching the operating mode
- CPU data, order number, serial number, versions
- Contents of the diagnostic buffer
- Information regarding the module status
- Acknowledge pending messages (alarms)
- Data for communication, such as IP address, MAC address, router
- View of watch tables
- Read/write tags
- Read/write tag status
- Firmware update
- Creating a program backup from the PLC or downloading a backup to the PLC

In addition to retrieving the status, the web server provides a user interface for maintenance actions on the automation system via the network. Access rights for each user are defined in a separate user administration.

8.5 Secure communication

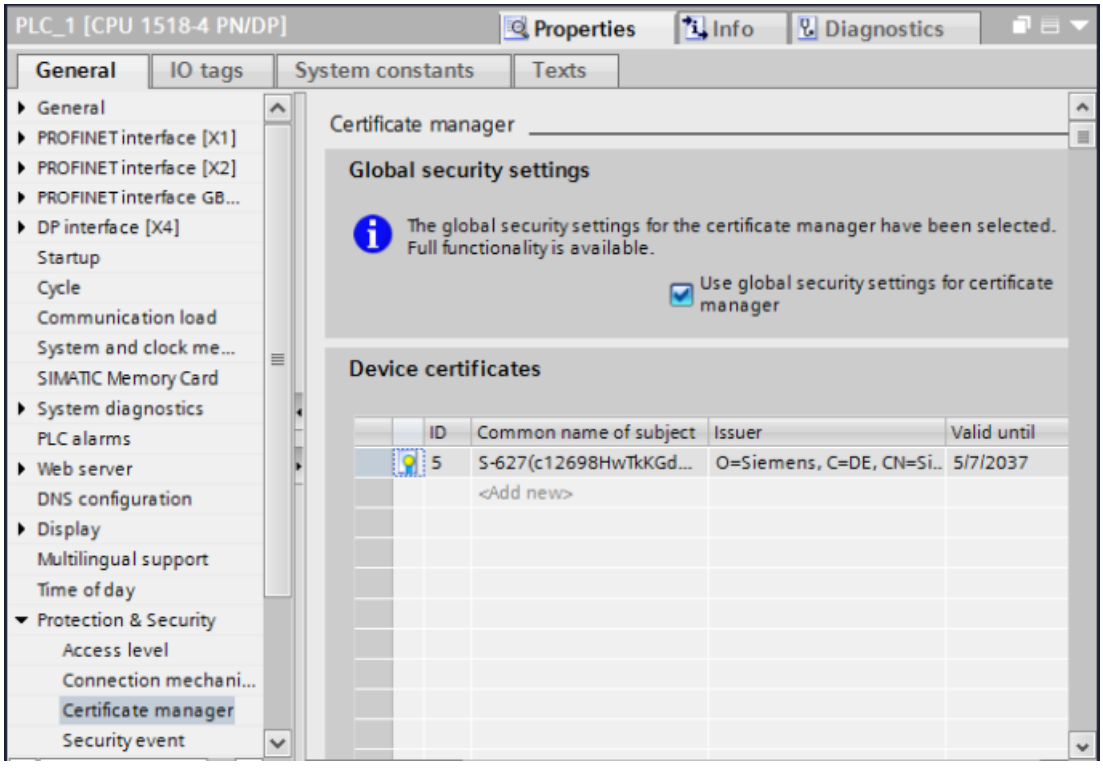
The term "Secure Communication" in STEP 7 (TIA Portal) describes the options for configuring a secure connection with HTTPS (http over TLS). When establishing a secure connection, both partners verify certificates that ensure confidentiality, data integrity, and endpoint authentication.

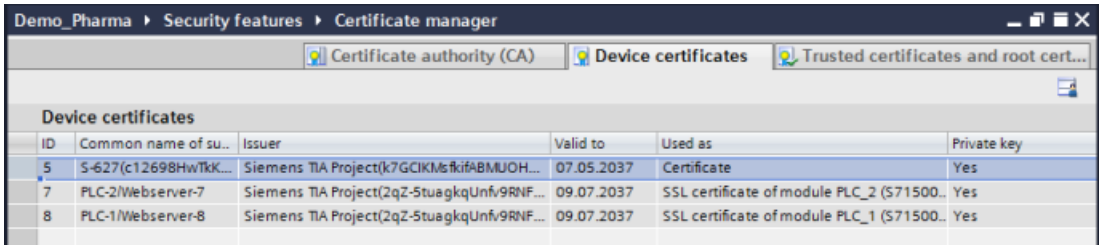
Digital certificates according to the X.509 standard can be created and signed by a trusted certification authority or the TIA Portal. Certificates created in the TIA Portal restrict functionality, but are sufficient for plant-internal communication.

Configuring a secure connection is recommended for the following applications:

- Access to the web server of the CPU
- Data exchange via Open User Communication (OUC) between two CPUs, CPU and TLS external device, for example, MES / ERP systems, CPU as e-mail client
- Data exchange using OPC UA

Each CPU has a local certificate manager. The cross-device certificate manager with global security settings should be used in a TIA Portal project with several CPUs. This provides an overview of all project-wide certificates with information on the issuer, validity and much else besides.



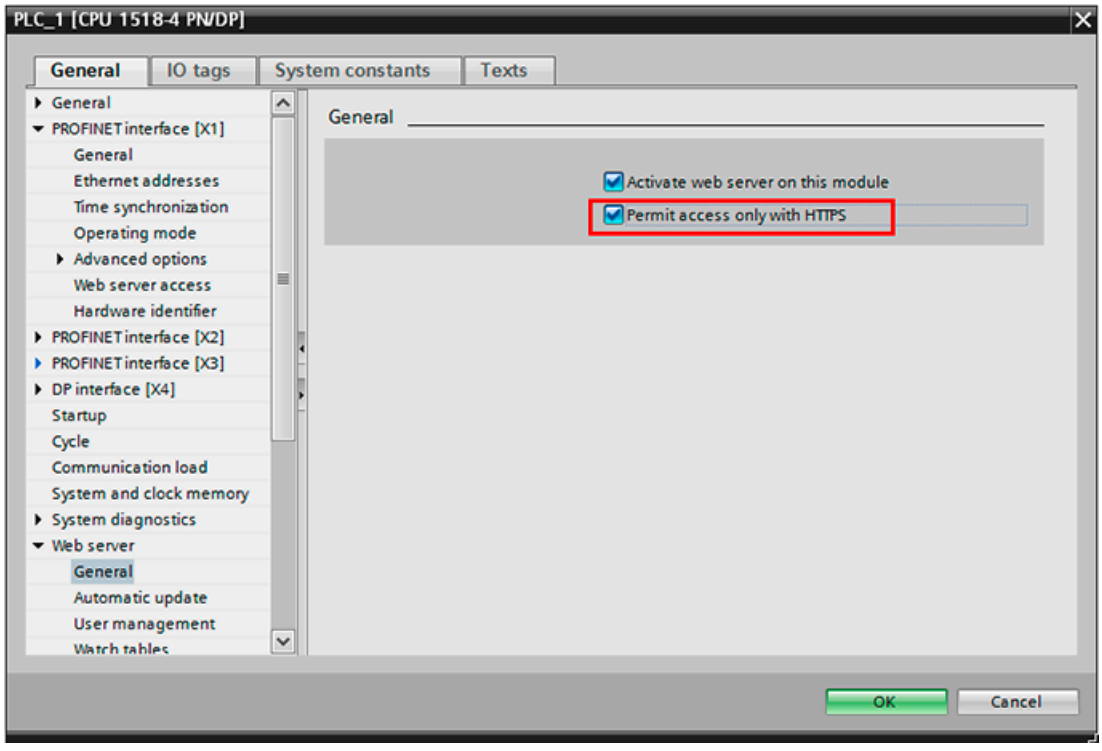


See also

- TIA Portal Information System > Editing devices and networks > Configuring devices and networks > Configuring networks > Secure communication (S7-1500)

8.5.1 Web access via a secure connection with HTTPS

A secure connection with HTTPS increases the security for the access to the web server of the CPU. A separate certificate is required for this, which the web server provides for download. The certificate is initially downloaded to the PC concerned via a connection with HTTP and added to the existing trusted certificates using the import function in the browser. The "Permit access only with HTTPS" property is then activated in the CPU properties. Now, only computers that have the required certificate are permitted to establish a connection.



See also

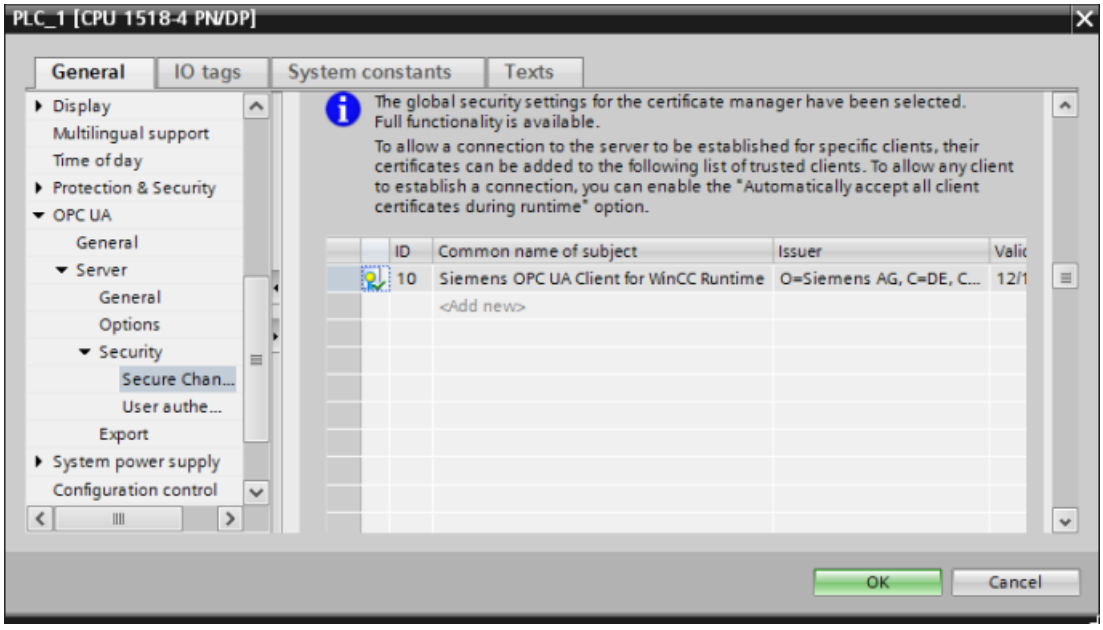
- TIA Portal Information System > Editing devices and networks > Configuring devices and networks > Creating configurations > Configuring automation systems (S7-300, S7-400, S7-1500) > Configuring a web server (…) > Standard websites (…) > Access only via HTTPS (…)

8.5.2 Data exchange using OPC UA

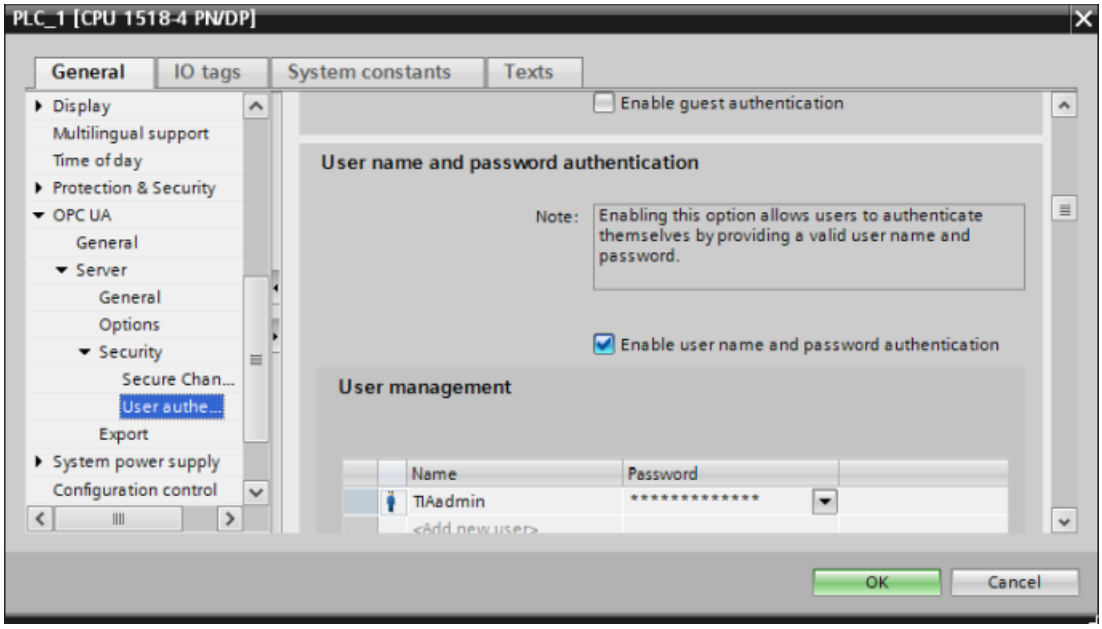
The S7-1500 CPU has an OPC UA server that provides tag contents for OPC UA clients. OPC UA (Unified Architecture) is a secure connection based on the exchange of certificates.

A configured project protection and the activation of the global security functions in the TIA Portal project are a requirement for the activation of the OPC UA server in the CPU.

The OPC UA server of the CPU provides a certificate that must be imported and accepted by the OPC UA client. The OPC client also has a certificate that is made known to the OPC UA server of the CPU by adding it to the list of certificates.



If the authentication of the OPC UA connection in the CPU is protected with user name and password, the OPC UA server also accepts this form of authentication for connection establishment. In this case, the setting "Automatically accept client certificates during runtime" can be activated later in the dialog.



If the connection was established successfully, the OPC UA client provides access to the values of the PLC and DB tags. The different value formats must be taken into consideration in the respective systems when transferring data.

For an offline configuration, the contents of the OPC UA server interface can be exported to an XML file.

See also

- TIA Portal Information System > Editing devices and networks > Configuring devices and networks > Creating configurations > Configuring automation systems (S7-300, S7-400, S7-1500) > Use OPC UA communication (S7-1500)
- System limits of the OPC UA server in SIMATIC S7-1500, Online Support under entry ID 109755846 (https://support.industry.siemens.com/cs/ww/en/view/109755846)

8.5.3 IP access protection

Various communication processors are also available to connect the SIMATIC S7-1500 to Industrial Ethernet (TCP / IP, ISO-on-TCP, UDP, S7 communication, etc.). These are used to extend the connection resources of the CPU. Compared to the Ethernet interfaces on the CPU, the CP 1543 communications processor in particular has additional security settings that prevent unauthorized connection of third-party devices.

After activating the security functions in the properties of the CP, only the configured communication partners are taken into account when establishing the connection. These are further S7 stations, NTP server for time synchronization, SMTP server for sending e-mail, DNS server, DHCP server, etc.

Access for selected partners is entered with the corresponding data, either in the IP Access Control List (ACL) or in the MAC Control List. The DHCP service autonomously manages the required IP addresses in the ACL.

See also

- TIA Portal Information System > Editing devices and networks > Configuring devices and networks > Additional information on configurations > Communication modules and network components > Industrial Ethernet / PROFINET > IP access protection

8.6 Diagnostic functions

8.6.1 Diagnostics in the TIA Portal engineering system

If the engineering system has an online connection to the PLC, detailed diagnostic information can be called up. In addition to the CPU, security modules, various modules and technology objects also provide comprehensive diagnostic information.

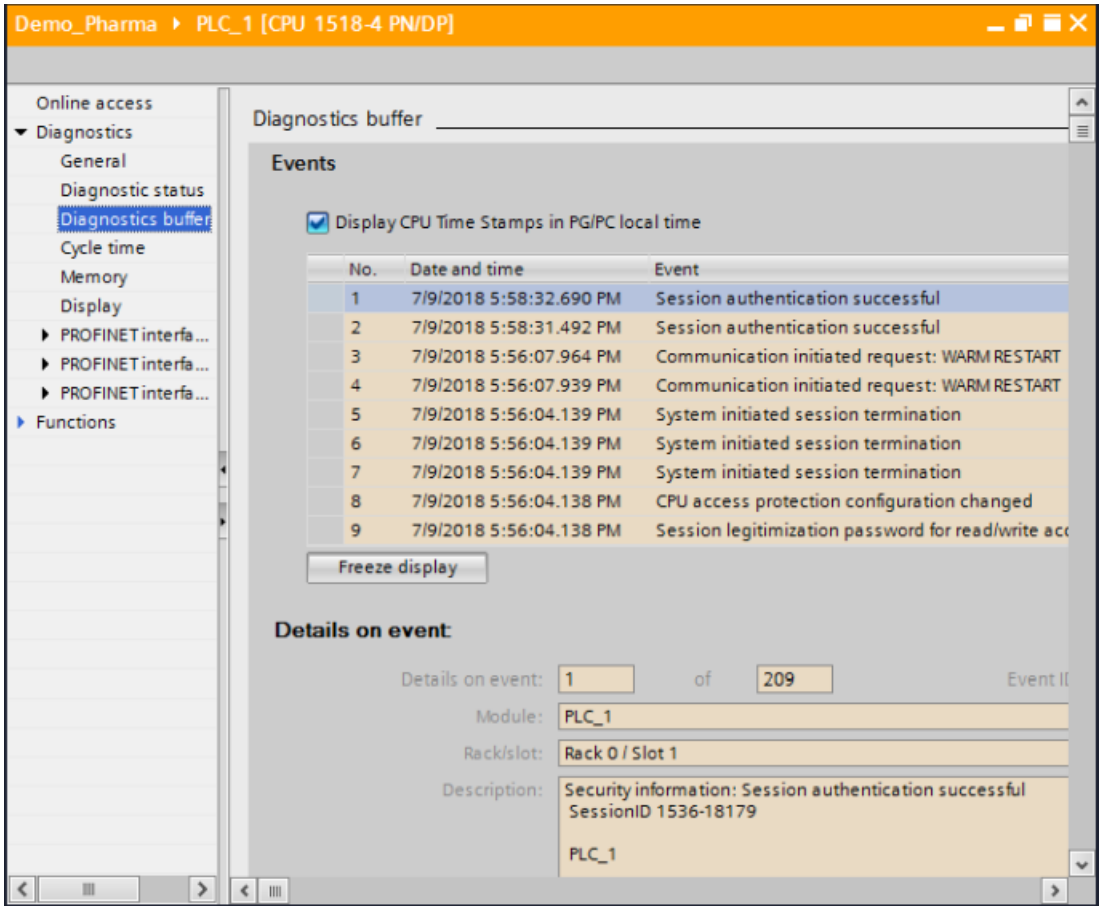
The diagnostics buffer in which all system events are recorded can also be output for a CPU, in addition to the general data such as order number, version, manufacturer information. Information is also shown regarding the operating status (RUN/STOP), memory utilization and cycle time.

Diagnostic buffer

The diagnostic buffer serves as a log file for all events that occur on the CPU and the assigned modules. Entries are made with time stamp and information text in the order of their occurrence. If required, the display can be frozen so that detailed analyses can be performed. Entries continue to be made in the background.

The diagnostic buffer can be read out in the following ways:

- In the TIA Portal engineering system using the Online & diagnostics entry, if an online connection exists.
- Using the display directly on the CPU
- Using the web server of the CPU, if it is activated.

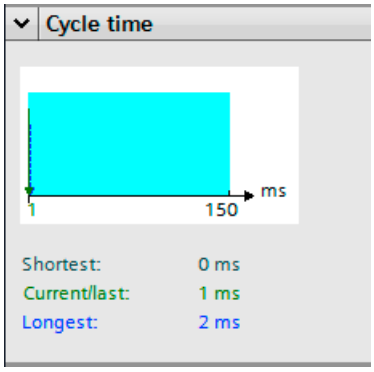


See also

- TIA-Portal Information System > Editing devices and networks > Device and network diagnostics > Hardware diagnostics > Checking a module for defects > Reading out the diagnostic buffer of a CPU

Cycle time

Under Online & diagnostics or on the "Online Tools" task card, a cycle time diagram can be opened if the TIA Portal engineering system has an online connection to the PLC.



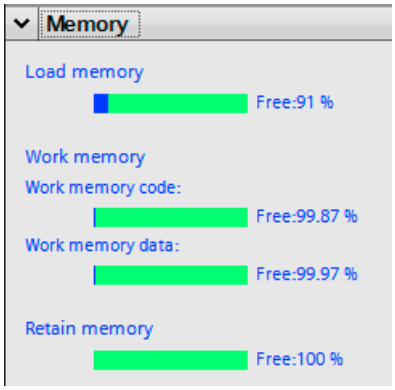
The diagram shows the following, starting from the last transition of STOP to RUN:

- The shortest cycle time
- The current cycle time
- The longest cycle time

The absolute values are displayed below the diagram.

Memory usage

Under Online & diagnostics or on the "Online Tools" task card, the memory usage can be called up if the TIA Portal engineering system has an online connection to the PLC.



8.6.2 diagnostics on the local display

The CPU S7-1500 has a display on which the device, status and diagnostic buffers can be called directly on the device and various settings can be made. The display provides the following functions:

- Overview of the PLC and memory card with order number, serial number, version, etc.
- Diagnostics with listing of alarms, diagnostic buffers and watch tables
- Settings for IP address (only after approval), date and time, change of operating mode (RUN/STOP switchover), memory reset and reset to factory settings; additional protection functions for the user program during RUN, see chapter "Local display protection (Page 165)"
- Module information for the plug-in hardware
- Display settings such as brightness, energy-saving and standby modes, language changeover separately for the operator interface and alarms

8.7 Test of the user program

The TIA Portal engineering system provides convenient functions for testing the user-specific program. If the hardware of the PLC is not available, it can be simulated with the PLCSIM or PLCSIM Advanced software package. Both software packages are part of the scope of delivery of SIMATIC STEP 7 (TIA Portal) Professional and are installed separately. Compared to PLCSIM, PLCSIM Advanced allows program testing in parallel for up to 4 CPUs communicating with each other over a TCP/IP network.

8.7.1 Simulation of the PLC using the PLCSIM software

The hardware of the PLC is simulated with PLCSIM. The application is opened as soon as the simulation for the selected PLC is started in the TIA Portal engineering system. The user program is downloaded to the software. Once RUN mode has been activated, the software simulates the program execution as in the PLC. The TIA Portal engineering system receives an online connection for the simulation so that the convenient test functions can be utilized.

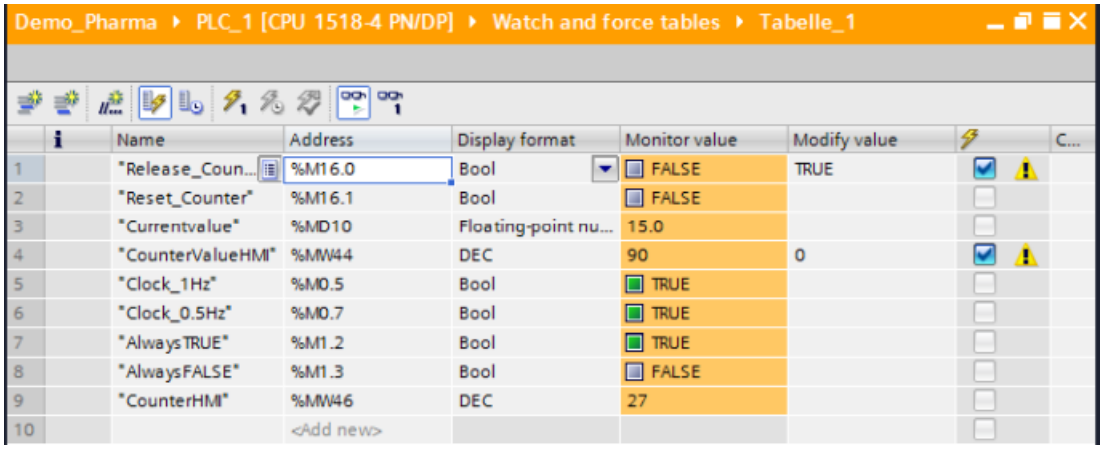
8.7.2 Testing with online connection

The online connection is established for the selected device in the project tree in the TIA Portal engineering system using the button or the shortcut menu, if the PLC hardware is available and accessible. Alternatively, the online connection is established by means of the simulation with PLCSIM. As soon as an online connection is available, extensive testing possibilities are offered:

- Online / offline comparison of complete programs, individual blocks, tag tables, hardware, etc.
  The comparison of software objects is based on checksums that are generated for specific data of the objects. Some objects (blocks, PLC tags/PLC data types) provide a detailed comparison.
- Online monitoring of the execution of individual blocks
- Testing with program status (definition of call environment and breakpoints)
- Watch and force tables for tracking value changes and modifying values
- Trace function for recording value changes over a definable time period

Watch and force tables in the engineering system

Relevant values can be assembled in tables in order to monitor value changes and specify values selectively.

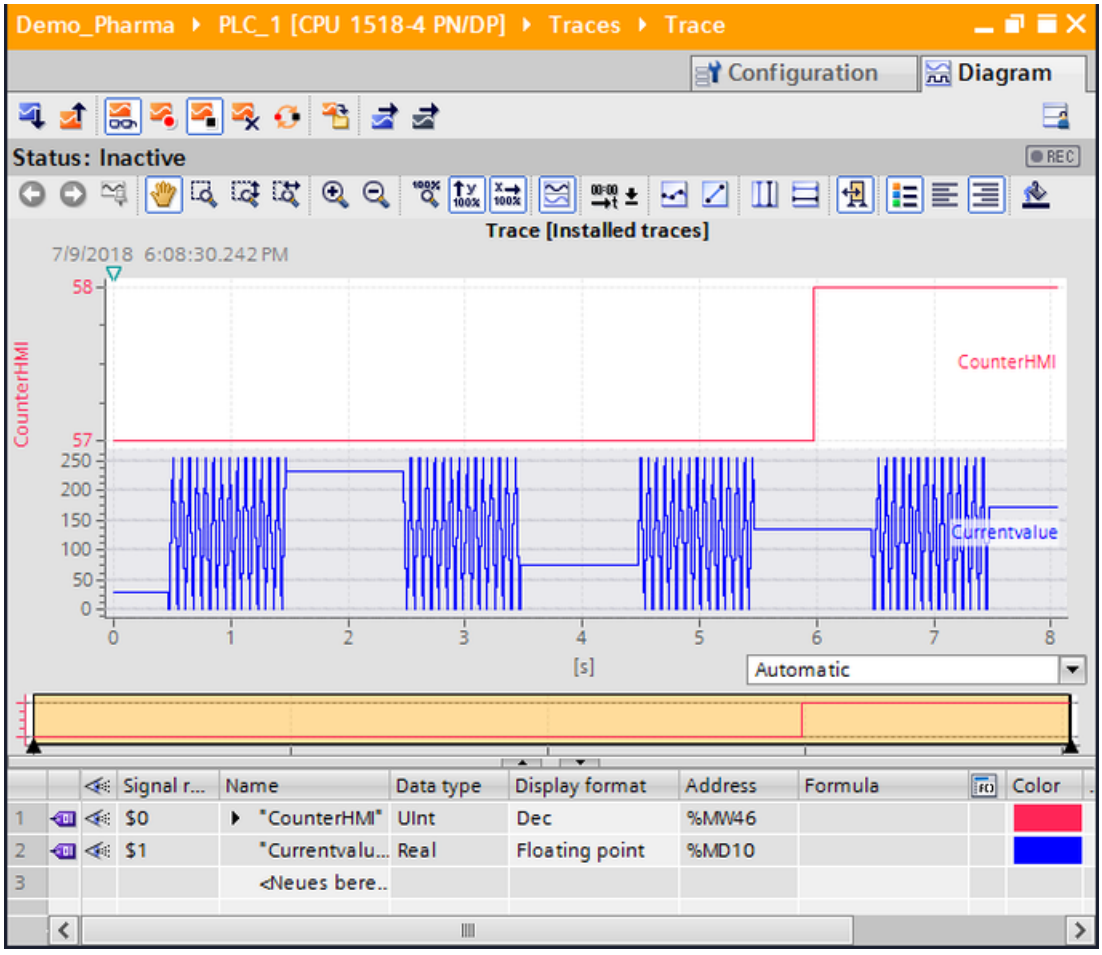


See also

- TIA Portal Information System > Programming a PLC > Testing a user program
- TIA Portal Information System > Programming a PLC > Comparing PLC programs > Comparing blocks

Trace function

The trace function is used for evaluating tag values for highly dynamic actions. The recordings can be saved and read out again if required. Active recordings of an axis control panel or PID controller can be added to the respective curve diagram.



See also

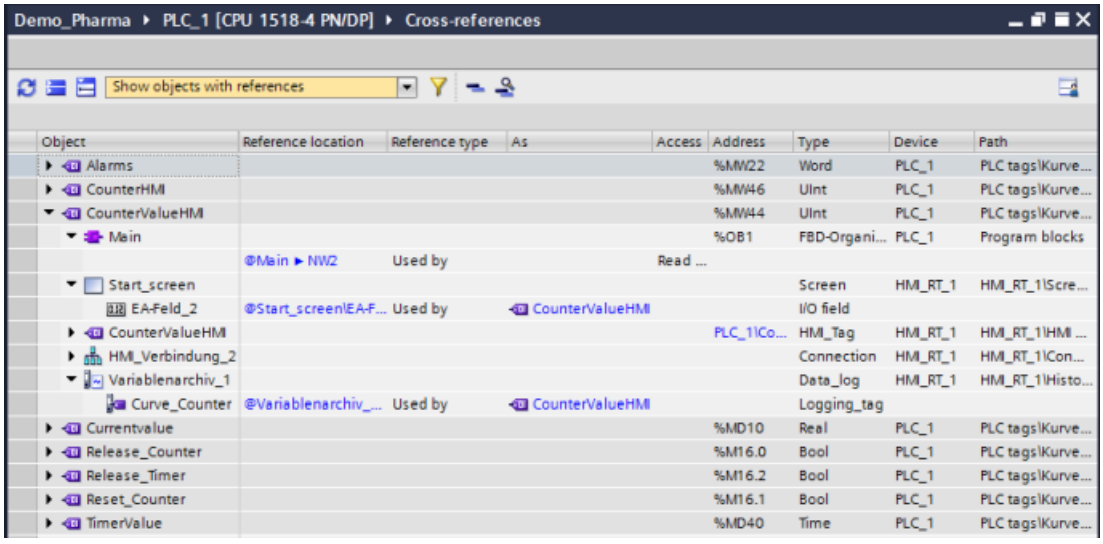
- TIA Portal Information System > Online and diagnostic functions > Using the trace and logic analyzer function
- Machine-level operator control and monitoring, Online Support under entry ID 93905586 (https://support.industry.siemens.com/cs/ww/en/view/93905586).

8.7.3 Cross-reference list

The cross-reference list also provides valuable information to test the user program. It provides an overview of the use and interdependence of the operands, blocks, tags, screens, etc. used within the project. Integrated links lead directly to the respective point of use.

The cross-reference list is generated for an object in the project tree and represents the points of use across devices for the entire TIA Portal project for the selected object. Lower-level objects as well as reference objects are listed in the same way.

The figure shows an example of the use of the PLC tag "CounterValueHMI" in the PLC and in the visualization.



Object	Reference location	Reference type	As	Access	Address	Type	Device	Path
Alarms					%MW22	Word	PLC_1	PLC tags\Kurve...
CounterHMI					%MW46	UInt	PLC_1	PLC tags\Kurve...
CounterValueHMI					%MW44	UInt	PLC_1	PLC tags\Kurve...
Main					%OB1	FBD-Organi...	PLC_1	Program blocks
	@Main ▸ NW2	Used by		Read ...				
Start_screen						Screen	HMI_RT_1	HMI_RT_1\Scre...
EA-Feld_2	@Start_screen\EA-F...	Used by	CounterValueHMI			I/O field		
CounterValueHMI					PLC_1\Co...	HMI_Tag	HMI_RT_1	HMI_RT_1\HMI ...
HMI_Verbindung_2						Connection	HMI_RT_1	HMI_RT_1\Con...
Variablenarchiv_1						Data_log	HMI_RT_1	HMI_RT_1\Histo...
Curve_Counter	@Variablenarchiv_...	Used by	CounterValueHMI			Logging_tag		
Currentvalue					%MD10	Real	PLC_1	PLC tags\Kurve...
Release_Counter					%M16.0	Bool	PLC_1	PLC tags\Kurve...
Release_Timer					%M16.2	Bool	PLC_1	PLC tags\Kurve...
Reset_Counter					%M16.1	Bool	PLC_1	PLC tags\Kurve...
TimerValue					%MD40	Time	PLC_1	PLC tags\Kurve...

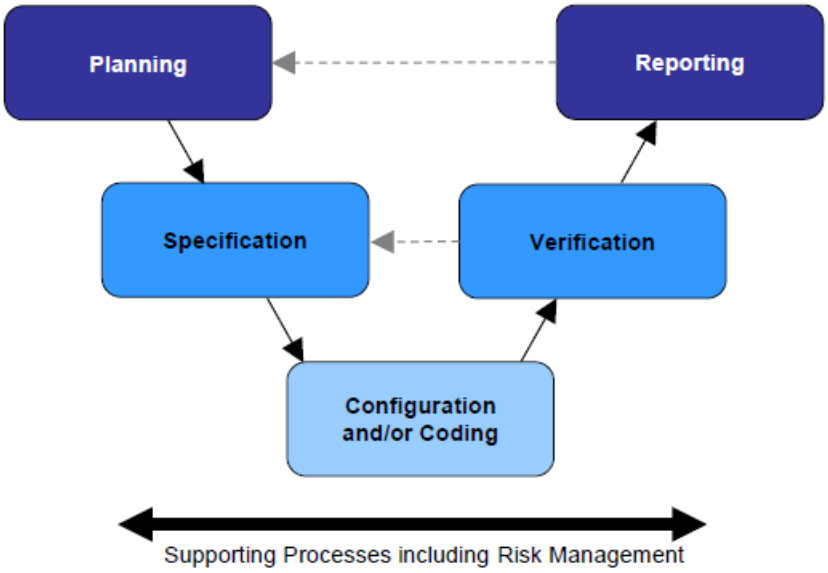
A definition of user-defined filters limits the display of cross-references to relevant areas. These filters can be saved, edited and deleted.

Complete project documentation also includes the cross-reference list.

Support for Verification

9

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

9.1 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)

9.2 Verification of hardware

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

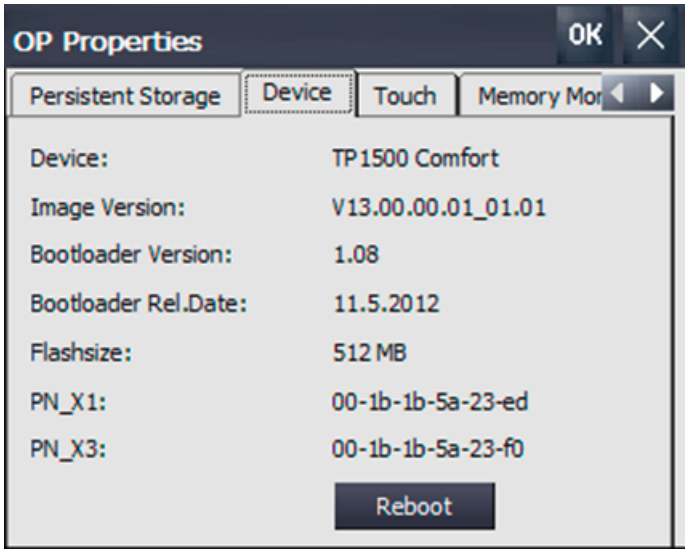
Utilities for the verification of the system hardware

- Printouts and screenshots as proof in the verification (see chapter "Documentation of the project data (Page 189)")
- Additional visual checks of the hardware when necessary
- Printouts of the hardware configuration and verification of compliance with the control cabinet documentation
- PC pass with information on all installed hardware and software components. This can be created manually or using commercially available tools.
  Where necessary, there should also be an additional visual check.

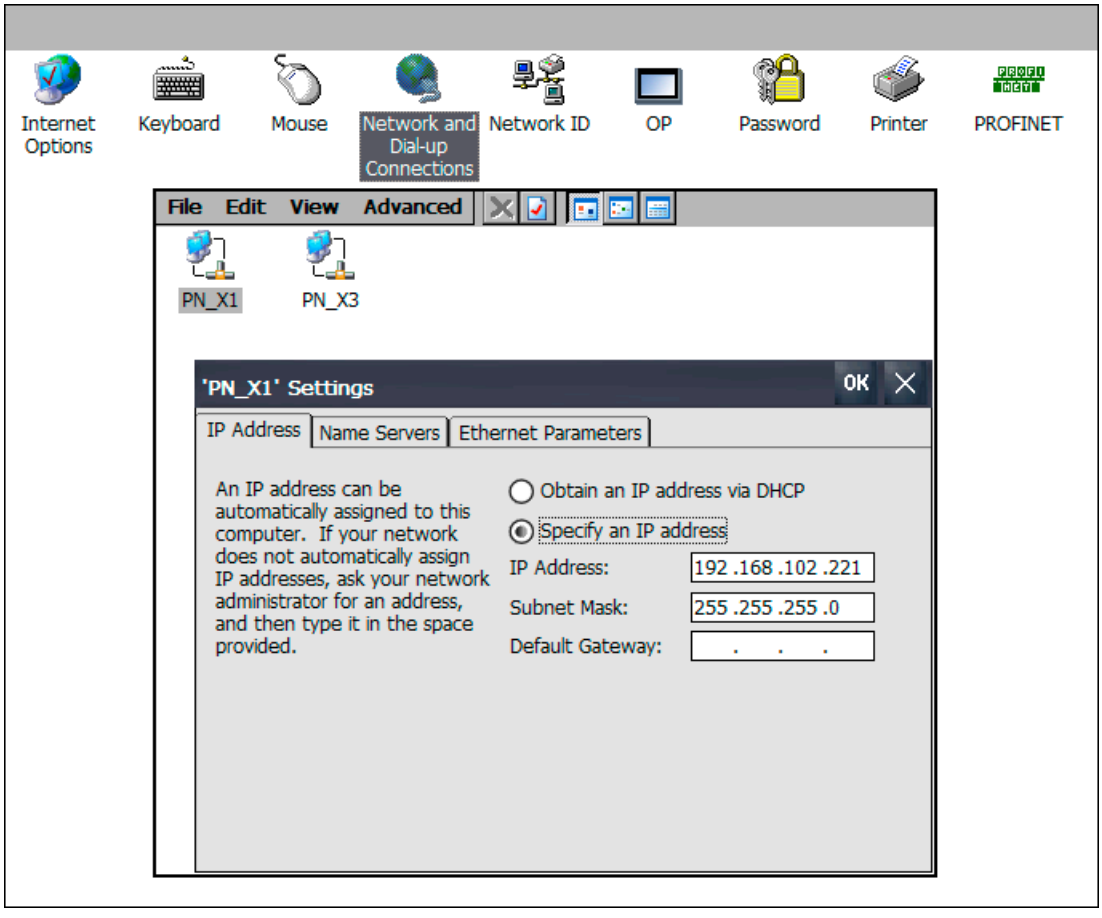
Verification of the panel hardware

Panels are delivered preconfigured with the Windows CE operating system. For the hardware verification, the panel type and version and the supplemental memory card and network configuration must be checked.

Panel type and version can be read out on the panel using Control Panel > OP.

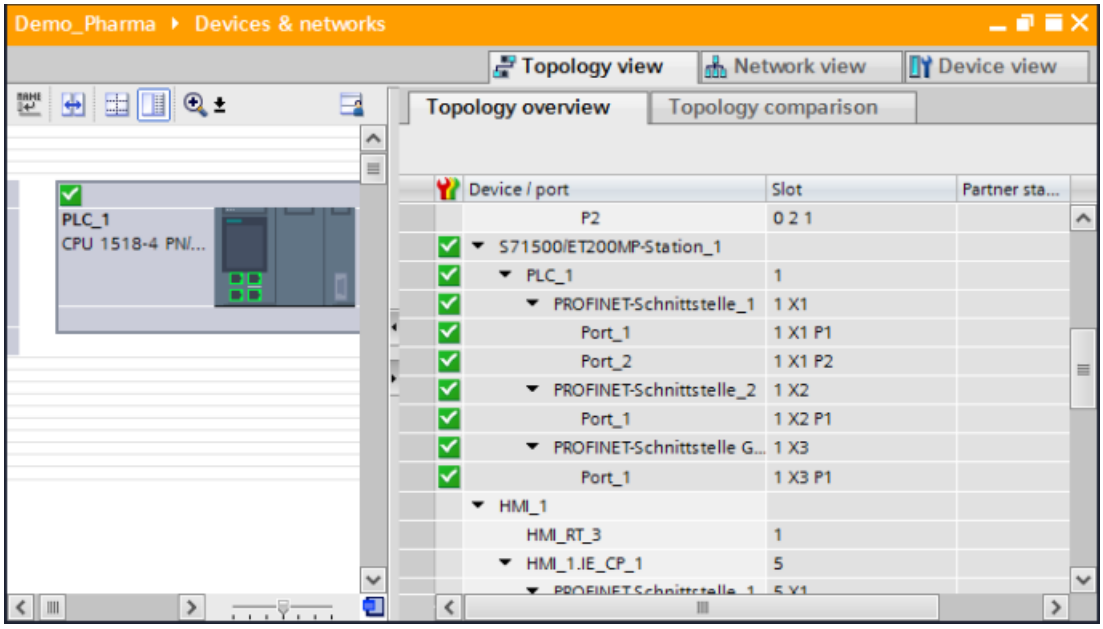


The network configuration is called using Control Panel > Network and Dial-up Connections.



Verification of the hardware for automation systems

An offline/online comparison is started in the topology overview of the Devices & networks editor. For devices with online connection, the hardware data is output in a table. The display of the columns can be expanded, if required.



9.3 Verification of software

Utilities for the verification of the system software

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

- Installed software, see chapter "Verification of software products (Page 185)"
- Documentation of the project data, see chapter "Documentation of the project data (Page 189)"
- Cross-reference list, see chapter "Cross-reference list (Page 179)"
- SIMATIC Security Controller, see chapter "Installation of the SIMATIC WinCC RT runtime software (Page 47)"
- Diagnostics of communication connections, see chapter "Diagnostics of communication connections (Page 115)"
- Memory space view, see chapter "Memory space view (Page 115)"
- Chapter "Diagnostics of the communication connection (Page 147)"
- Diagnostics of PLC status, see chapter "Diagnostic functions (Page 174)"

- Memory usage of the PLC, see chapter "Online & diagnostics in the TIA Portal engineering system (Page 174)"
- Chapter "Test of the user program (Page 177)"

9.3.1 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.

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

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

Configuration based on the installed products, libraries, blocks, etc., then corresponds to category 4.

If "Free code" is also programmed, this corresponds to a category 5.

Procedure for category 5 functions

Here, specification and testing requires a much greater effort:

1. Creation of a description of functions for the software
2. Definition of the functions used
3. Definition of the inputs and outputs used
4. Definition of the operator control and monitoring ability
5. Software design according to specification and programming guidelines
6. Structural testing for compliance with programming guidelines
7. Functional testing for conformity with description of functions
8. Approval prior to use or duplication

9.3.2 Verification of software products

For the verification of "standard" software products used, a check is made to verify whether the installed software meets the requirements of the specification. These are usually products that are not designed specifically for a customer but rather are freely available on the market, e.g.:

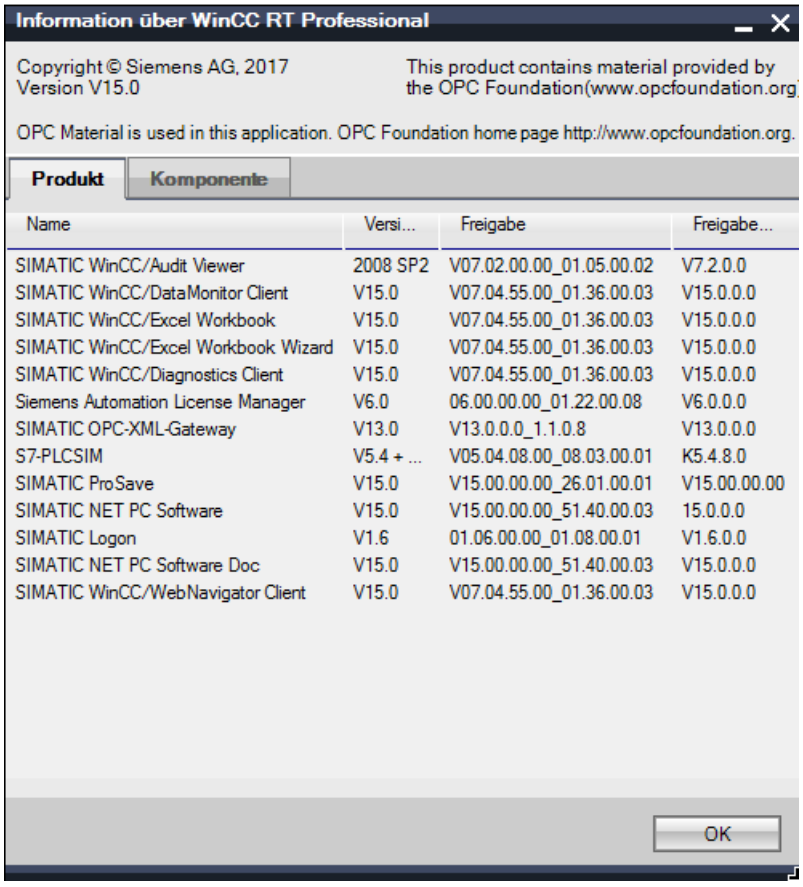
- Operating system and other software packages
- SIMATIC WinCC Runtime system software
- SIMATIC standard options (DataMonitor, WebNavigator, Recipes, etc.)

- SIMATIC WinCC Premium Add-ons (PM-CONTROL, PM-QUALITY, PM-OPEN IMPORT, PM-ANALYZE)
- Standard libraries

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

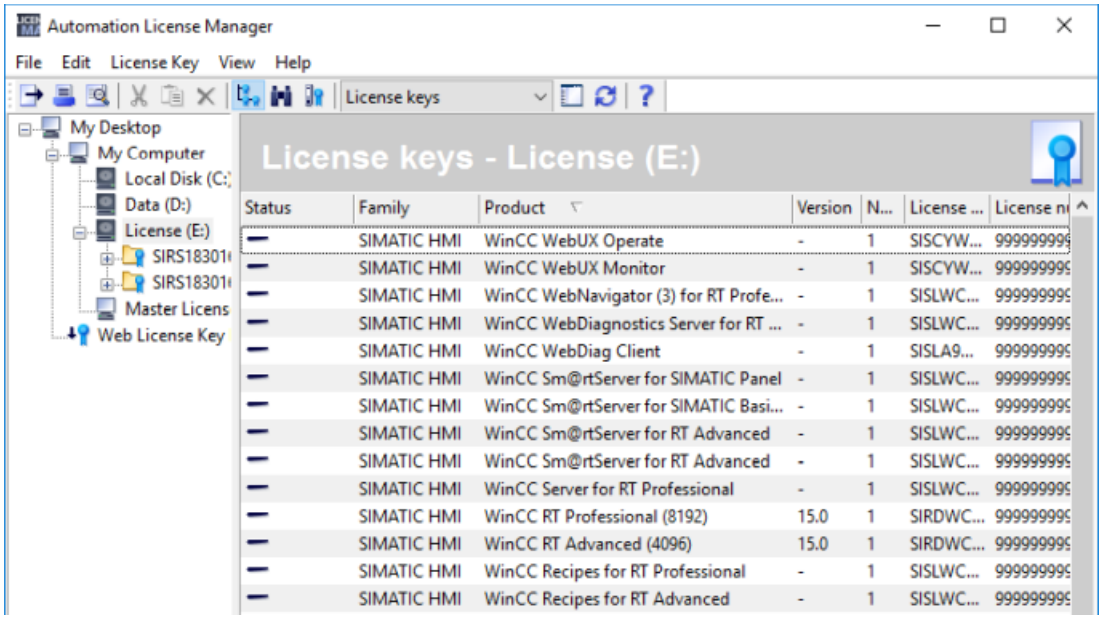
- The settings in the Windows operating system required for the WinCC system software can be queried in the SIMATIC Security Controller application: All programs > Siemens Automation > Security Controller > Accepted settings (see also chapter "Installation of the SIMATIC WinCC RT runtime software (Page 47)")

The installed SIMATIC software is documented in detail in the WinCC RT Start application under Help > About WinCC RT Start ... > Components.



Name	Versi...	Freigabe	Freigabe...
SIMATIC WinCC/Audit Viewer	2008 SP2	V07.02.00.00_01.05.00.02	V7.2.0.0
SIMATIC WinCC/DataMonitor Client	V15.0	V07.04.55.00_01.36.00.03	V15.0.0.0
SIMATIC WinCC/Excel Workbook	V15.0	V07.04.55.00_01.36.00.03	V15.0.0.0
SIMATIC WinCC/Excel Workbook Wizard	V15.0	V07.04.55.00_01.36.00.03	V15.0.0.0
SIMATIC WinCC/Diagnostics Client	V15.0	V07.04.55.00_01.36.00.03	V15.0.0.0
Siemens Automation License Manager	V6.0	06.00.00.00_01.22.00.08	V6.0.0.0
SIMATIC OPC-XML-Gateway	V13.0	V13.0.0.0_1.1.0.8	V13.0.0.0
S7-PLCSIM	V5.4 + ...	V05.04.08.00_08.03.00.01	K5.4.8.0
SIMATIC ProSave	V15.0	V15.00.00.00_26.01.00.01	V15.00.00.00
SIMATIC NET PC Software	V15.0	V15.00.00.00_51.40.00.03	15.0.0.0
SIMATIC Logon	V1.6	01.06.00.00_01.08.00.01	V1.6.0.0
SIMATIC NET PC Software Doc	V15.0	V15.00.00.00_51.40.00.03	V15.0.0.0
SIMATIC WinCC/WebNavigator Client	V15.0	V07.04.55.00_01.36.00.03	V15.0.0.0

The **Automation License Manager** program provides information about the licenses installed on each WinCC computer.

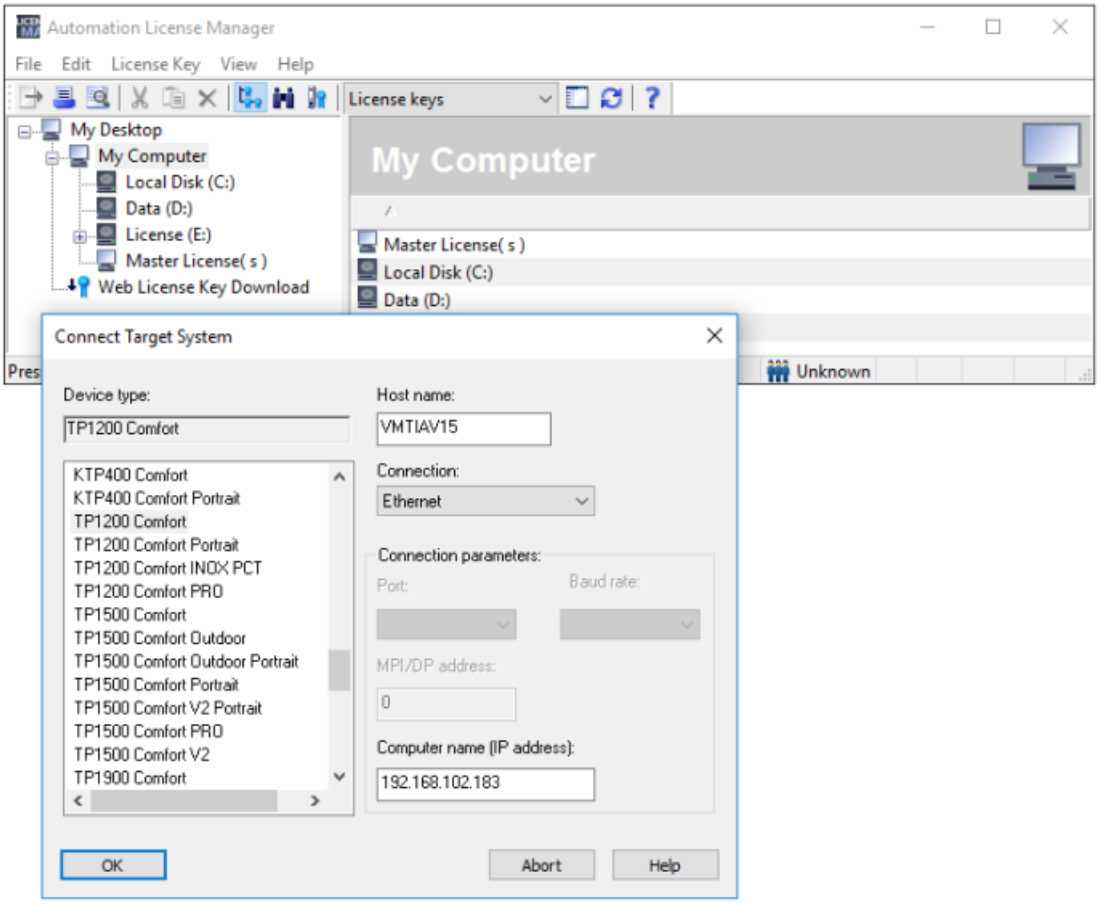


Verification of the software for panels

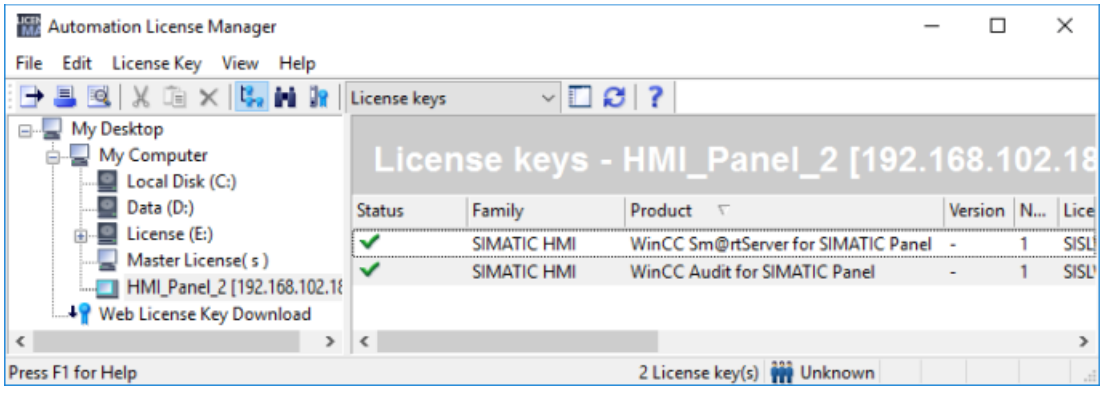
The installed operating system version is read out for panel under Control Panel > System. The available memory is also shown here:

The Automation License Manager program can also be used to verify the SIMATIC licenses installed on panels. For this purpose, a connection between the panel and Automation License Manager is established:

- With TIA Portal engineering system
  using the shortcut menu HMI Device maintenance > Authorize/License
- Without TIA Portal engineering system
  in Automation License Manager using the menu Edit > Connect target system > Connect HMI device



Below is an example of installed licenses on a panel:



9.3.3 Verification of the application software

For verification of the application software, test descriptions are generated according to the requirements of the software specification and then used as a basis for testing the software.

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 with other devices (controllers, MES systems, etc.)
- Inputs and outputs
- Control modules (control module level)
- Equipment phases and equipment operations (technical functions)
- Relationships between modes (MANUAL/AUTOMATIC switchovers, interlocks, start, running, stopped, aborting, completed, etc.)
- Process tag designations
- Visualization structure (P&ID)
- Operating philosophy (access control, group rights, user rights)
- Archiving concepts (cyclic storage, long-term archives)
- Alarm concept
- Trends
- Time synchronization

Configuration data such as the tags, blocks, functions or graphics used can be output based on reports. For this purpose, ready-made standard layouts and print jobs exist in the global library of the TIA Portal engineering system, see chapter "Reporting of process and production data (Page 111)".

9.4 Documentation of the project data

Documentation of the project data can be created in the engineering system in support of the hardware and software verification. For this purpose, the TIA Portal provides a number of templates in the global library, also in accordance with the ISO standard for technical project documentation.

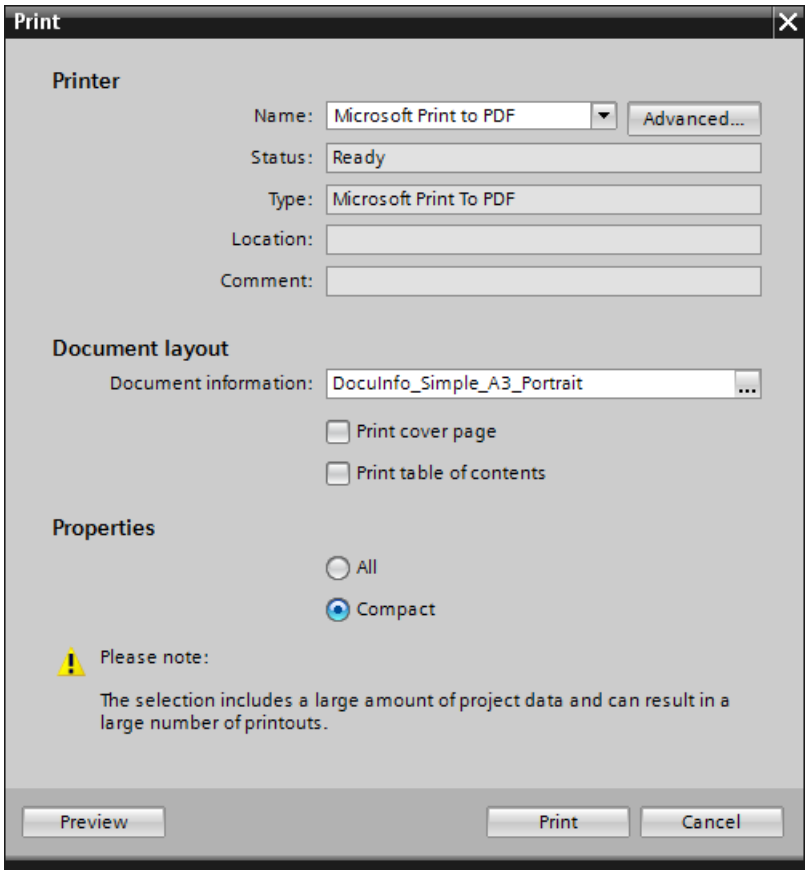
Documentation of the following data can be displayed as a print preview on the screen or output on a printer via the corresponding shortcut menu:

- Complete project data when the top node is selected in the project tree
- Project data for a device in the project tree
- Contents of an open editor (e.g. Devices & networks)
- Tables
- Libraries

See also

- TIA Portal Information System > Editing projects > Editing project data > Printing project contents

In the print dialog box, the printer, document layout and the extent of the documentation, either "All" or "Compact", is selected. The printing of previously selected objects is also offered.



9.5 Configuration control

9.5.1 Project versioning

In a storage concept, it is specified, for example, that the project is backed up following a change. The TIA Portal provides the following options:

- Minimizing and copying the project data to another directory
- Archiving the project data in compressed form as a file with extension .zap[Vx].

Both when minimizing and when archived, the project data is reduced to the essential components, thereby reducing the file size.

When minimized, a project copy is created in a selected directory. It is suitable for sending by e-mail or for archiving with a standard tool such as Winzip.

Project archives created with the TIA Portal can be extracted again in the TIA Portal. Version compatibilities must be taken into consideration.

A version ID can, for example, be included in the file name.

See also

- TIA Portal Information System > Editing projects > Creating and managing projects > Archiving and retrieving projects

Versioning of data in WinCC options / Add-ons

Make sure that the appropriate databases are backed up if the Premium Add-ons are used such as PM-CONTROL / PM-QUALITY. Before the data backup, the project must be closed in PM-SERVER and the utility application for PM-CONTROL and PM-QUALITY to disconnect the databases from the MS SQL Server.

The directory that contains the project data of the add-ons (by default: C:\Users\Public \Documents\Siemens\ProcessManagement\...) is copied or packaged at which time a version number can be integrated in the name. 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 Project.CSV is saved to the configured storage location.

9.5.2 Change control of the configuration data

The configuration can be controlled using the versioning of the individual configuration elements and the associated change documentation, see chapter "Versioning of the application software (Page 87)".

Data Backup 10

10.1 Backing up the operating system and SIMATIC WinCC

The backup of the operating system and the WinCC installation should be carried out with hard drive images. These images allow you to restore the original state of PCs without significant effort.

Note

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

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

10.2 Backup for the Comfort Panel

For a Comfort Panel, a data backup can be saved to a USB stick or SD card.

The backup contains the following data:

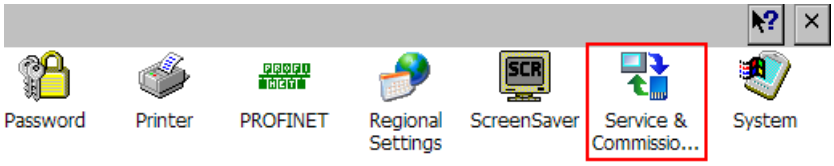
- Operating system
- Compiled Runtime software
- Recipes
- User administration
- Configuration data (licenses, add-ons, third-party files)

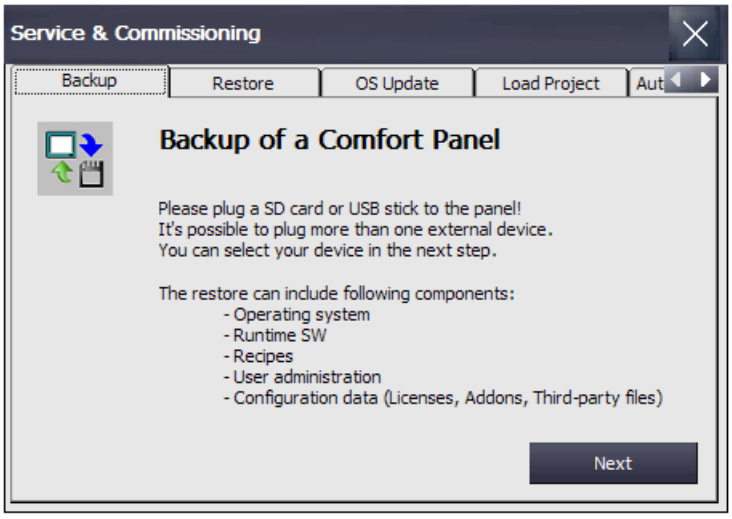
The backup and restoration of the data is performed using the Service & Commissioning object in the Control Panel. The OS Update via USB stick or SD card is also supported.

The created backups can be listed with time stamp and backup version number in the TIA Portal. For this, the memory card is connected to the configuration PC using a card reader, or the USB stick to the USB port, and the data is displayed in the TIA Portal using the Card Reader / USB memory editor.

Besides the manual backup, the Service & Commissioning object also provides an automatic backup function. The comfort panel has a second memory card slot for this. The slot is intended for a SIMATIC Memory Card (SMC) with at least 2 GB memory. If the automatic backup is activated, the backup is also updated automatically on the SMC at every project transfer.

This SIMATIC Memory Card (SMC) can be inserted in a different device of the same type. During booting, the SMC is read and the image is transferred to the device.





10.3 Backup of the automation software

A hardware and software upload to the TIA Portal engineering system from an automation system can be performed if RUN mode is activated and the device is accessible over the network (accessible devices button). The upload is started using the menu "Online > Upload device as new station (hardware and software)". The project data received can be backed up and logged as described in chapter "Project versioning (Page 190)".

Note

The PLC must be protected with protection level "No access" so that the project data cannot be downloaded from anywhere in the network.

See also

- Chapter "Protection levels (Page 160)"

Operation, Maintenance and Service 11

11.1 Operation and monitoring

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

The production can be monitored, operated and optimized using numerous interfaces. Screen signals in graphic and operating screens as well as trends, alarms, horns, etc., serve as central components for monitoring during operation. WinCC Professional also provides the display of a sequence status (GRAPH7) with the S7GraphOverview control and the mapping of a network from the PLC in an operating screen without STEP 7 installation with the PLC Code Display control.

See also

- TIA Portal Information System > Visualize processes > Interfaces > Runtime API (RT Professional) > Functions for displaying of PLC Code (…) > Display in the PLC code Display (…)

Runtime data can be output by the system based on reports. Corresponding reports and print jobs are configured in the engineering system for this purpose (see chapters "Reporting of process and production data (Page 111)" and "Output of process and production data (Page 142)").

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.

11.2 Operational change control

Changes to validated and operational plants must always be planned in consultation with the process owner, documented and only be implemented and tested after approval.

The example below illustrates the procedure for changes:

1. Initiation and approval of change specification by process owner
2. Description of the software change
3. Backup of the current WinCC project data
4. Implementation of software changes including manual documentation based on the current version
5. Test of changes including documentation
6. Backup the changed WinCC project data with the versioning

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

11.3 System restoration

The procedure described in this chapter should enable the end user to restore the operating system and the automation system after a disaster.

Disasters are taken to mean the following cases:

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

The system is restored using the backed up data. The backed up data (medium) and all the materials needed for the restoration (basic system, installation software, documentation) must be stored at a defined location. There must be a disaster recovery plan which must be checked on a regular basis.

Restoring the operating system and installed software

The restoration of the operating system and installed software is carried out by importing the corresponding images (see chapter "Data Backup (Page 193)"). The instructions provided by the relevant software supplier for the data backup application should be followed.

Restoring the application software

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

- Reading back the data from a manually created backup

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 view historical data in WinCC Runtime, corresponding backup versions with extensions mdf and ldf are copied back to the local computer and connected to the MS SQL Server via the Connect archive button in the controls for displaying the data.

11.4 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 stops 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 high priority are, for example:

- Automation system (AS)
- Network components

- Archive server
- WinCC server
- WinCC clients
- Panels

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

The following must also be noted:

- Configuration of alarming for power failure
- Specification of the time frame for shutting down the PC
- Specification of the time frame of the UPS battery backup

System Updates and Migration 12

12.1 Update of the system software

An update of the system software of a validated plant must be coordinated with or initiated by the user. An update such as this represents a system change, which must be planned and executed in accordance with the applicable change procedure. Similar to the description in chapter "Operational change control (Page 195)", this roughly means the following steps:

- Describe the planned change
- Effects on functions / plant units / documentation taking into consideration the system description of the new and modified functions in the readme file/release notes
- Impact on readability and availability of archived data
- Evaluate the risks to the overall process and the validated state
- Define the tests that need to be performed to maintain the validated status, based on the risk evaluation
- Approve/reject the change (in accordance with defined responsibilities)
- Update of existing system and preparation of test documents
- Perform data backup before update
- Implementation of the change in accordance with the manufacturer's instructions (after enabling of the plant)
- Accompanying documentation of the activities to be carried out
- Verification: Carry out and document the necessary tests
- Perform new data backup, possibly with system image

In considering possible influences, the following may be relevant:

- Process screens, objects, especially the script-based dynamization
- Alarm system and process value archiving in terms of function and display
- Access authorizations
- Interfaces
- Effects during download
- System performance
- Documentation (specifications)
- Verification tests to be repeated or performed for the first time

Note

Support for software update and project migration is provided by SIMATIC Product Support (http://support.industry.siemens.com)

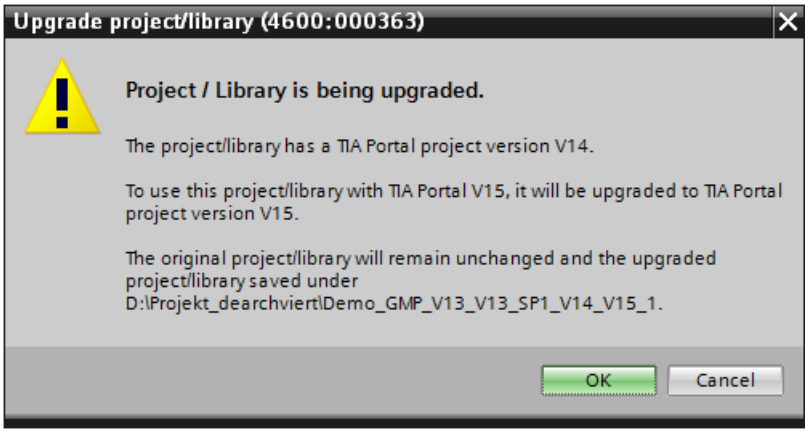
A list of the released Windows updates, e.g., for security gaps, is published in the Online Support under entry ID 18752994 (https://support.industry.siemens.com/cs/ww/en/view/18752994).

The application example under "Creating a WSUS (Microsoft Windows Server Update Service) with WinCC Systems" shows the configuration when Windows is operated in service mode, online support under entry ID 109754089 (https://support.industry.siemens.com/cs/ww/en/view/109754089)

Support for the operating system update on operator panels, Online Support under entry ID 19701610 (https://support.industry.siemens.com/cs/ww/en/view/19701610).

12.2 Upgrading TIA projects

Upgrading a TIA project depends on the compatibility of the various TIA versions. A TIA project that was created with the direct predecessor version is automatically upgraded to the new version when it is opened in the current TIA Portal version after confirmation of a query. The project hereby receives a new file extension in which the new version number is coded (* .ap[version number]).



Projects from older TIA Portal versions can not be upgraded directly, instead they require a step-by-step upgrade.

See also

- TIA Portal Information System > Editing projects > Compatibility of projects > Compatibility between TIA Portal versions

Procedure for the upgrade:

- A dialog with instructions for upgrading appears when you open a TIA Portal project with the previous version. After a positive confirmation, the upgrade is started automatically.
- Information and error messages regarding the upgrade are output in the information area and can be processed as appropriate.
- Hardware and software must be compiled for each individual device at the conclusion of an upgrade.
- PC systems of the type WinCC Professional / WinCC Client are automatically upgraded to the new version.
- For devices of the type HMI (Panels) or PC systems of the type RT Advanced, the old device version is retained during the migration. The device can be exchanged for a device with the current version via the "Device/Version" property. It can be decided separately for each device whether a version change to the current version is to be carried out.

Note

Changing the device version deletes all data on the HMI device. Therefore, the runtime data should be saved on the HMI device before the device version is changed.

The project history over different TIA Portal versions is shown in the project properties.

Blocks with know-how protection

Blocks with know-how protection are not automatically upgraded to a new TIA Portal version. However, the blocks can be downloaded to the controller and are executable. If the blocks are to be opened and edited in the new TIA Portal version, the know-how protection must be removed before the upgrading. The know-how protection is linked to the TIA Portal version and can only be removed in the same TIA Portal version in which it was set up. Following the upgrade, the know-how protection can be re-established for the affected blocks.

Global libraries

Global libraries are managed outside the project data and therefore not automatically upgraded. If the contents are still to be used, these must be upgraded separately.

Instruction version

Instructions may be available in different versions if your project has been edited in different product versions. The TIA Portal provides the option to upgrade the project and instructions to the latest version. The new instruction versions will be available afterwards but will not be used automatically in the program.

See also

- TIA Portal Information System > Editing projects > Compatibility of projects > Upgrading projects
- TIA Portal Information System > Editing projects > Compatibility of projects > Upgrading projects > General information on upgrading

12.3 Migration of the application software

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

On the basis of a system analysis, risk analysis as well as the respective boundary conditions (existing installed base, default plant downtimes, etc.) an individually adjusted migration strategy is designed taking into account the necessary qualification measures. The system update activities described in chapter "Update of the system software (Page 199)" must also be taken into consideration.

The technical understanding of the individual steps, whether manual or automated, and the consideration of possible error cases are the basic requirements for a successful and efficient validation strategy. Therefore, it is particularly important to involve the appropriate competent professionals in the planning.

See also

- GAMP 5 Guide, Appendix D7 "Data Migration"
- GAMP 5 Guide, Appendix S4 "Patch and Update Management"

12.3.1 Migration of the project data for HMI devices

With a migration, the WinCC project data from WinCC classic or WinCC flexible is converted to the data format for WinCC (TIA Portal) and can then be further processed there.

Before the migration, the WinCC versions that are released from a migration must be checked. The project being migrated may have to be upgraded to the required version.

Procedure for migration:

- The project is converted to a migration format using the "Migration Tool" application. If the required WinCC flexible version is installed in parallel with the TIA Portal, the migration can be performed directly in the TIA Portal. This also applies to the parallel installation of the corresponding SIMATIC STEP 7 version.
- The migration is started in the TIA Portal in the portal view via the migration button or in the project view via the menu Projects > Migrate project.
- During the migration, the devices that are no longer supported are automatically replaced by comparable successor devices. Configuration settings are offered for conversion of the screen format.
- Hardware and software must be compiled for each individual device at the conclusion of a migration.

The migration report shows the migration sequence. Compilation information for the individual devices is output in the information area and may require further post processing.

If adjustments are made in the project, these are subject to validation.

The validation effort is decided in consultation with the process owner. Possible check points are the new features available in WinCC as well as the correct installation of the software components required for migration according to the instructions.

See also

- TIA Portal Information System > Migrate projects and programs > Migrate projects to a TIA Portal project
- Migration of plants with SIMATIC (TIA Portal) – Visualization, Online Support under entry ID 76878921 (https://support.industry.siemens.com/cs/ww/en/view/76878921)
- Migration of plants with SIMATIC (TIA Portal) – Complete systems, Online Support under entry ID 83558085 (https://support.industry.siemens.com/cs/ww/en/view/83558085)

12.3.2 Migration of STEP 7 projects

STEP 7 projects of type SIMATIC STEP 7 V5.4 SP5 or higher can be migrated to a TIA Portal project. The migration of integrated projects is also supported.

In general, all configurations and objects that are supported by the current TIA Portal version are migrated.

- Devices from the S7-300 and S7-400 family
- Profibus configurations with distributed I/O.
- Blocks in LAD, FBD or STL, S7-SCL and S7-GRAPH
- PLC tags
- User-defined data types (UDT)
- Interrupts and much more

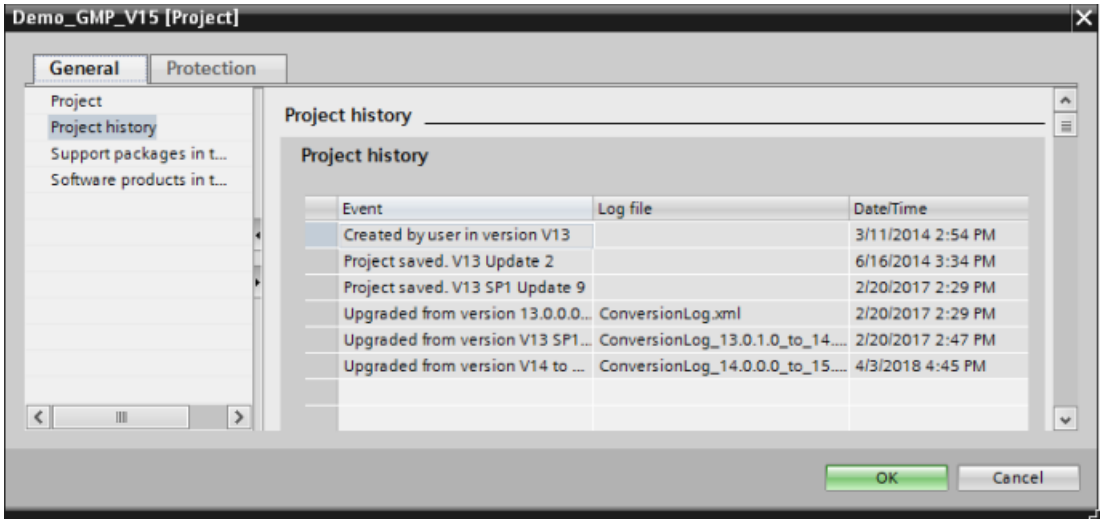
During migration, the software configuration is taken into account by default. If it can be ensured that the hardware is covered by equivalent products in the TIA Portal, the hardware configuration can also be included. Otherwise, non-specific devices will be used during the migration, which will later be replaced by the corresponding hardware. Network configurations and connections must also be manually updated.

See also

- TIA Portal Information System > Migrate projects and programs > Migrate projects to a TIA Portal project > Migrate STEP 7 programs (S7-300, S7-400)> Migrate STEP 7 projects (S7-300, S7-400)

A consistent initial project is a requirement for a successful migration of a STEP 7 project into a TIA Portal project. A guide to checking the consistency can be found in Online Support under entry ID 5416540 (https://support.industry.siemens.com/cs/ww/en/view/5416540).

Alarms, information and errors are entered in a migration report. This report can be viewed at any time in the project tree at the highest project node under Properties > Project history.



After the migration, a compilation is required. Additional information and any errors in the software are output during compilation. If the software has been compiled error-free, the data can be downloaded to the CPU.

See also

- Entries for migration to STEP 7 (TIA Portal) and WinCC (TIA Portal), Online Support under entry ID 56314851 (https://support.industry.siemens.com/cs/ww/en/view/56314851)
- Requirements for migration of a STEP 7 V5.x project to a STEP 7 Professional (TIA Portal) project, Online Support under entry ID 62100731 (https://support.industry.siemens.com/cs/ww/en/view/56314851)
- Migration of plants with SIMATIC (TIA Portal) controllers, Online Support under entry ID 83557459 (https://support.industry.siemens.com/cs/ww/en/view/83557459)

12.3.3 Migrating PLC programs

Within the TIA Portal, PLC programs can be migrated, for example from the device families S7-300 and S7-400 to an S7-1500. During the PLC migration, a new CPU S7-1500 is created in addition. The project data will be adapted to the new CPU during migration and copied to the new device. Program structures are hereby adapted and instructions are updated. The old CPU remains available unchanged.

See also

- TIA Portal Information System > Migrating PLC programs to an S7-1500-CPU / ET 200SP > Basics of migrating PLC programs (S7-1500)
- TIA Portal Information System > Migrating PLC programs to an S7-1500 CPU / ET 200SP> Special features of the migration

12.4 Validation effort for migration

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

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

- Change request of the user,
  see chapter "Operational change control (Page 195)"
- Migration plan or update plan
- Checklist for the installation / migration
- Test specification to ensure functionality after upgrading
- Test results together with attachments and deviations
- Concluding report

The migration functionality made available by the system is a product property that does not require more testing in detail in the project application. For each migration, a migration log is created containing information about changed project components. This migration log should be checked carefully. Changes that impact GMP critical functions must be given special consideration.

Note

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

Checkpoints in the verification

To verify the changes made, the following checkpoints may be relevant in the test specification:

- Installation of required software components according to instructions.
- New or changed system functions of this version
- Basic functionalities of the system, from a technical and user perspective
- GMP-critical functions and parameters, archiving and reports, as well as the readability of archived data
- Automated migration sample testing (see above note about migration functionality in the product)
- Manual adjustments made in addition to automatic migration must be described separately, their implementation documented and adequately tested.

The steps in chapter "Update of the system software (Page 199)" should be taken into consideration.

Note

A renewed (documented) check of the program sequence in a corresponding test environment is required in particular when migrating PLC programs in which the program structure and instructions are adapted. The scope of this validation must be agreed with the process owner.

Abbreviations

A

Abbreviation	Description
CFR	Code of Federal Regulations
CP	Communication Processor
DS	Design Specification
FAT	Factory Acceptance Test
FB	Function block
FC	Functions
FDA	Food and Drug Administration
FS	Functional Specification
GAMP	Good Automated Manufacturing Practice
GMP	Good Manufacturing Practice
HDS	Hardware Design Specification
HMI	Human Machine Interface
HW	Hardware
IPE	Inter Project Engineering
IQ	Installation Qualification
OLE	Object Linking and Embedding
OPC	OLE for Process Control
OQ	Operational Qualification
PLC	Programmable Logic Controller
RT	Runtime
SAT	Site Acceptance Test
SCADA	Supervisory Control and Data Acquisition
SDS	Software Design Specification
SMC	SIMATIC memory card
SW	Software
URS	User Requirement Specification
UPS	Uninterruptible power supply
UTC	Universal Time Coordinated

Index

L

M

N

O

P

R

S

T

U

V

W

Further information

E-Mail:
pharma@siemens.com

Internet:
www.siemens.com/pharma

Siemens AG
Process Industries and Drives
Pharmaceutical and Life
Science Industry
76181 Karlsruhe
GERMANY

A5E44854710-AA

Siemens
Pharma Industry

www.siemens.com/automation