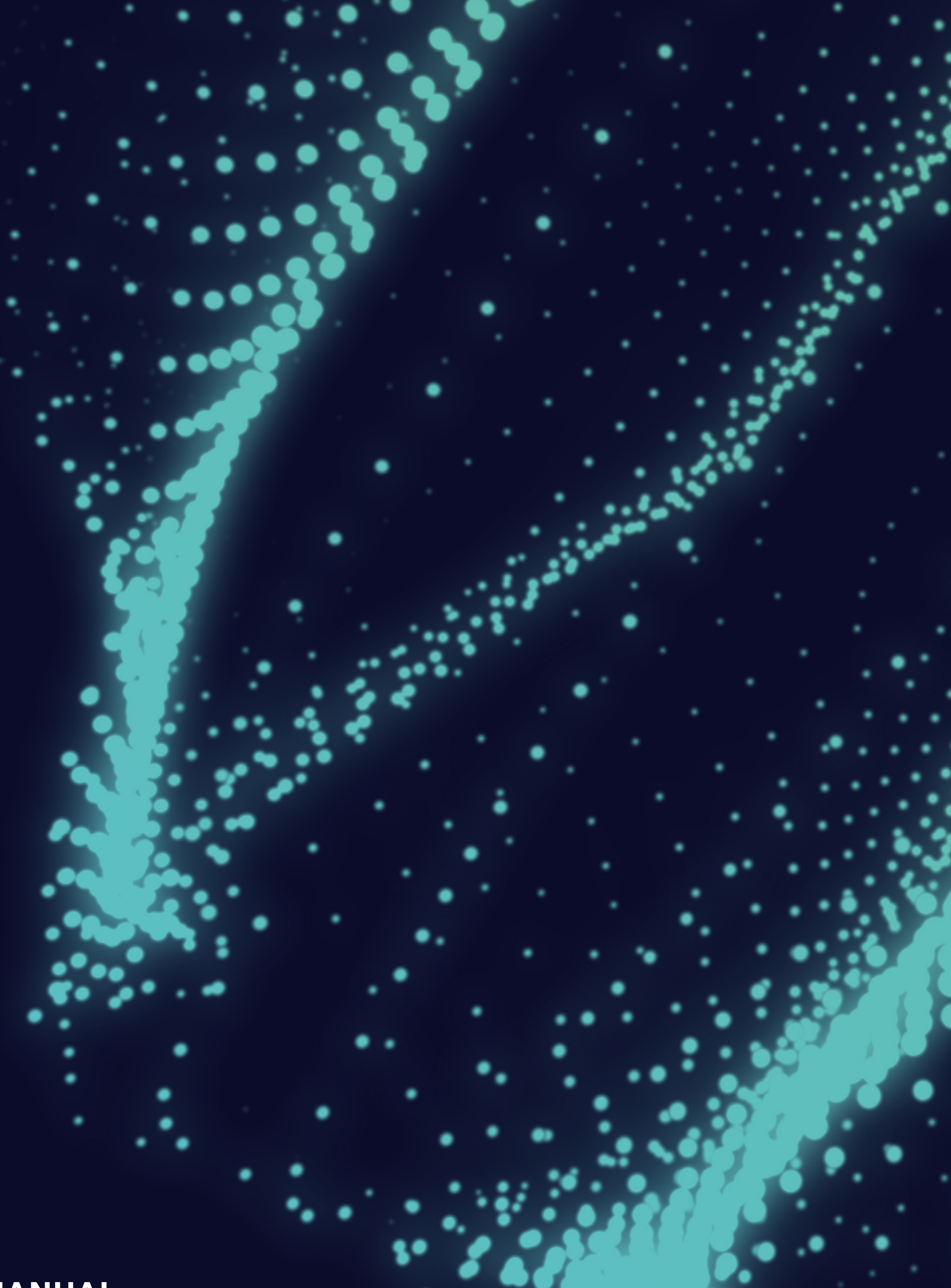
SIEMENS



Edition 05/2022

GMP ENGINEERING MANUAL

SIMATIC

SIMATIC PCS 7 V9.1

Guidelines for Implementing Automation Projects in a GMP Environment
siemens.com/pharma

SIEMENS

SIMATIC

SIMATIC PCS 7 V9.1 GMP Engineering Manual

Configuration Manual

Guidelines for Implementing Automation Projects in a GMP Environment

05/2022
A5E42888188-AB

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
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E42888188-AB
Ⓟ 05/2022 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 about SIMATIC PCS 7 is required to understand this manual. Knowledge of GMP as practiced in the pharmaceutical industry is also an advantage.

Validity of this manual

The information in this manual applies to SIMATIC PCS 7 V9.1. The components examined are PCS 7 ES, PCS 7 OS and SIMATIC BATCH. Refer to the product catalog or compatibility tool for detailed information on the compatibility of the individual components.

- SIMATIC PCS 7 Product Catalog (https://support.industry.siemens.com/cs/de/en/view/109745632)
- Compatibility tool (www.siemens.com/kompatool)

Any questions about the compatibility of the add-on products for SIMATIC PCS 7 should be addressed directly to the suppliers.

Industry Mall catalog and ordering system – Add-on products for SIMATIC PCS 7 (https://mall.industry.siemens.com/mall/en/de/Catalog/Products/10008888?tree=CatalogTree)

Position in the information landscape

The system documentation of the SIMATIC PCS 7 Process Control System is an integral part of the SIMATIC PCS 7 system software. It is available to every user in the Plant and User Documentation Manager (PUD Manager) or online as PDF.

This manual supplements the existing SIMATIC PCS 7 manuals. It is not only useful during configuration, it also provides an overview of the requirements for configuration and what is expected of computer systems in a GMP environment.

Structure of this manual

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

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

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

Training centers

Siemens offers a number of training courses to familiarize you with SIMATIC PCS 7. Please contact your regional training center, or the central training center in D 90327 Nuremberg, Germany.

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

Siemens on the Internet

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

SIMATIC PCS 7 technical documentation (https://support.industry.siemens.com/cs/ww/en/view/109794065)

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

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

Technical support on the Internet

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

Industry Online Support offers there for example:

- Manuals and product information
- FAQs and application examples

You can also find on this page:

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

Additional support

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

Find your personal contact partner at: (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:

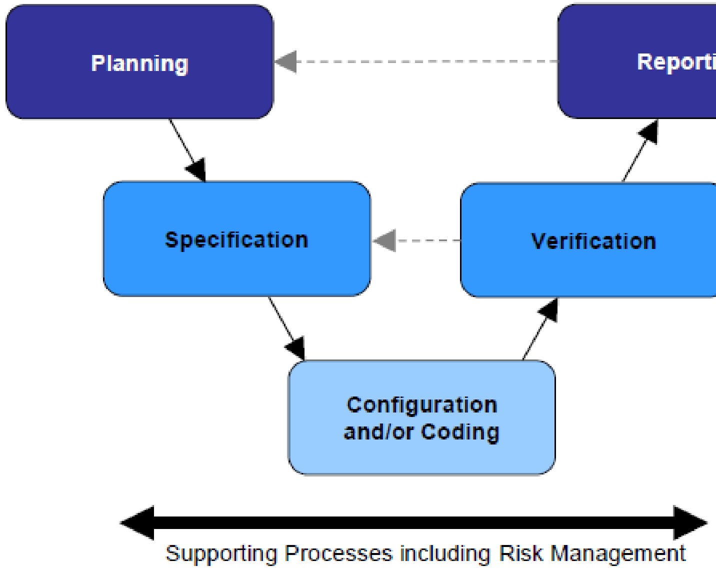
Title (Author)	Subtitle	Area of application
21 CFR Part 11 (US Food and Drug Administration, FDA)	Electronic Records, Electronic Signatures	Law/regulation for manufacturers and importers of pharmaceutical products for the U.S. market
Annex 11 of the EU GMP Guide (European Commission)	Computerised systems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


Planning
Reporting
Specification
Verification
Configuration and/or Coding
Supporting Processes including Risk Management

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 a GMP Environment 2

This chapter describes the essential requirements an automated system in the GMP environment must meet regarding the use of computerized systems. These requirements must be defined in the specification and implemented during configuration. In case of subsequent changes or interventions in the system, reliable evidence must be provided at all times, regarding who, at what time, and what was changed or implemented. The requirements for this task are implemented in various functions and described in the following chapters.

Note

This chapter describes the general requirements for computerized systems. How to meet these requirements with a specific system is dealt with starting from chapter "System Specification (Page 25)".

2.1 Categorization of hardware and software

Hardware categorization

According to the GAMP 5 Guide, hardware components of a system fall into two categories "standard hardware components" (category 1) and "custom built hardware components" (category 2).

Software categorization

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

2.2 Test effort depending on the categorization

The effort involved in validation (specification and testing) is much greater when using configured and, in particular, customized products compared to the effort for standard products (hardware and/or software). The overall effort for validation can therefore be significantly reduced by extensive use of standard products.

2.3 Change and configuration management

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

The procedure includes, for example:

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

See also

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

2.4 Software creation

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

Use of type/instance concepts and copy templates

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

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

Identification of software modules/types/copy templates

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

Changes to software modules/types/copy templates

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

2.5 Access control and user administration

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

- Combination of unique user ID and password; see also chapter "Requirements for user IDs and passwords" (Page 19)
- RFID / smart cards together with a password
- Evaluation of biometrics, e.g. fingerprint scanners

2.5.1 Applying access control to a system

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

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

Note

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

2.5.2 Requirements for user IDs and passwords

User ID:

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

Password:

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

- Use of uppercase letters
- Use of lowercase letters

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

See also

- Chapter "Setting up user administration (Page 41)"

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 by the operator to be traced back to the original data. A secure audit trail is particularly important when GMP-relevant electronic records are created, modified or deleted.

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

2.9 Reporting batch data

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

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

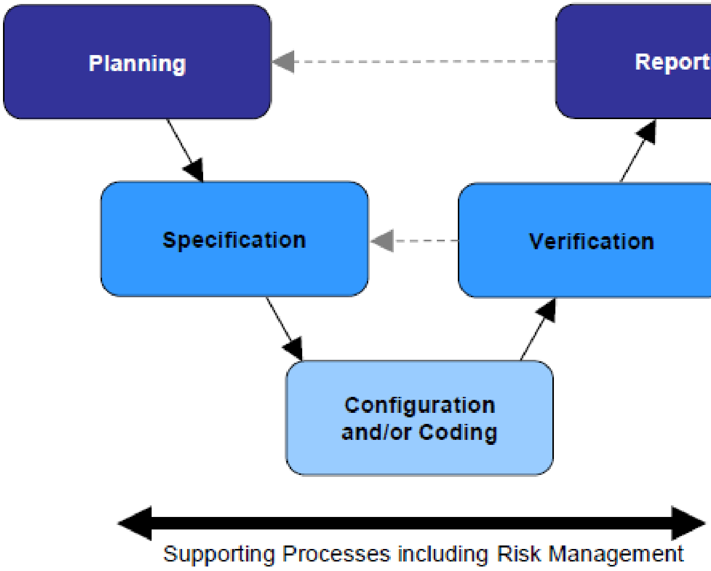
- GAMP 5 Guide, Appendix M2 "Supplier Assessment"

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.


Planning
Reporting
Specification
Verification
Configuration and/or Coding
Supporting Processes including Risk Management

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)
- General configuration and design (system design, general topics)
- Hardware (and network) design specification (HDS)
- Software design specification (SDS)
- HMI specification

A very good overview of the PCS 7 portfolio as well as for optimized processing of projects from planning to implementation and testing, all the way to handover to the customer is also offered by the following article. However, this article is only available inside the Siemens organization.

- Multimedia-based demonstration system "Fast-Track-Engineering", Online Support under entry ID 60242433 (https://support.industry.siemens.com/cs/ww/en/view/60242433)

3.1 Selection and specification of the hardware

Various system designs are used for the automation as well as the operation and monitoring of simple and complex production processes and manufacturing operations.

The selection of hardware components should be measured against the requirements. These requirements may be of a functional nature, but may also include aspects such as local conditions, compatible software or data security.

3.1.1 Hardware specification

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

- Hardware overview diagram, system structure and organization
- Control cabinets (control cabinet names, UPS configuration, location), PC station control cabinets, automation system with CPUs, I/O cards, etc.
- PC components for server and client
- Installation procedures and instructions for servers, clients, ES
- Appropriate subdivision of plant and plant unit areas for the AS
- Network structure for Industrial Ethernet, e.g. switches, transmission technology (electrical, optical, wireless), names and Ethernet configuration of the stations (AS, PC stations, etc.), general network settings
- Profibus/Profinet installation, division of networks for the automation systems, and specific Profibus/Profinet settings
- Time synchronization, if hardware components are involved
- Barcode scanner configuration
- Field devices

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

Note

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

See also

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

3.1.2 Selecting the hardware components

Use of hardware components from the PCS 7 catalog ensures the long-term availability of hardware and spare parts.

For reasons of system availability and data security/integrity, an appropriate class RAID systems for PC components, such as ES, OS single stations, OS servers and BATCH servers should be implemented in the system design.

When a **SIMATIC PCS 7 bundle** is supplied, the customer receives a PC on which all software required for the relevant applications is installed. The components contained in the bundle are not always identical to the products of the same names available on the market. As a consequence, the availability of spare parts will differ too.

In virtual systems, too, you should prefer well-proven system components, such as ESXi server.

Note

Only hardware from the current PCS 7 catalog should be used. The use of unreleased configurations requires additional effort for specification and test phase. See Product Catalog (https://support.industry.siemens.com/cs/de/en/view/109745632).

If PCs are placed in control cabinets, it must be ensured that suitable hardware components are provided, such as operator channel extensions.

There are different types of automation systems.

- **Standard automation system**
- **Fault-tolerant automation system**
  The user programs loaded in both CPUs are fully identical and are run synchronously by both CPUs. The switchover has no effect on the ongoing process because it is bumpless.
- **Fail-safe automation system**
  It automatically brings the plant to a safe state in the event of a fault. The relevant national regulations must be observed when configuring, commissioning, and operating fail-safe systems. S7 F-systems provide a reference sum of the fail-safe program section available. This sum is recorded to enable the detection of changes in the fail-safe program.

See also

- Manual "PCS 7 PC Configuration", Online Support under entry ID 109794377 (https://support.industry.siemens.com/cs/ww/en/view/109794377)

3.1.3 CPU 410 for process automation

The "CPU 410-5H Process Automation" is specifically designed for the SIMATIC PCS 7 control system. As with previous controllers of the SIMATIC PCS 7 system, the CPU 410-5H Process Automation can be used in all process automation industries. The very flexible scalability based on PCS 7 process objects makes it possible to cover the entire performance range from the smallest to the largest controller, in standard, fault-tolerant and fail-safe applications with only one hardware.

This yields the following benefits:

- Reduced number of CPU versions, no memory cards
- Resulting in fewer spare parts
- Easy system and functionality extension
- Flexible area of application, increased ruggedness

See also

- Manual "PCS 7 CPU 410 Process Automation", Online Support under entry ID 109801828 (https://support.industry.siemens.com/cs/ww/en/view/109801828)

3.1.4 Hardware solutions for special automation tasks

Additional device-specific solutions are required to integrate hardware components which are not offered in the SIMATIC hardware manager. These components are interfaced using special device master data. Integration examples for such hardware components include:

- Integration of weighing modules (SIWAREX)
- Integration of frequency inverters for drives (Masterdrives, Micromaster)
- Integration of user-specific field devices

To keep validation work to a minimum, hardware components from the PCS 7 Add-on catalog (ST PCS 7 AO) should be given preference.

3.2 Security of the plant network

In the field of modern process control systems, the boundaries between the office and automation environments are disappearing at an ever increasing rate. Automation solutions with connected WEB clients, MES applications, and customized office networks and applications are growing in importance. To satisfy these demands and ensure as high a level of data security as possible, the planning and structure of networked PCS 7 automation solutions are highly important.

Measures for increasing data and plant security

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

- Staggered user, group, and role concept
- Safety concepts for network security and limited access to network drives
- SIMATIC Security Control (SSC)
- SCALANCE S firewall and VPN modules

For additional information, see also

- Chapter "Information security and data integrity (Page 53)"
- "Industrial 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 109780811 (https://support.industry.siemens.com/cs/ww/en/view/109780811)
- Manual "PCS 7 Compendium Part F – Industrial Security", Online Support under entry ID 109804118 (https://support.industry.siemens.com/cs/ww/en/view/109804118)

3.3 Specification of the basic software

The Software Design Specification (SDS) describes the software's architecture and configuration. This describes not only the application software but also the "standard" software components used in the system, for example by specifying the name, version number etc. This description serves as a reference when performing subsequent tests (FAT, SAT, etc.).

Commercially available standard software components include automation software components and software provided by third parties; see also chapter "Verification of software (Page 138)".

Hardware and software requirements and operating system selection

- Compatibility tool (www.siemens.com/kompatool)
- PCS 7 Toolset DVD, Readme file
- Manual "PCS 7 PC Configuration", Online Support under entry ID 109794377 (https://support.industry.siemens.com/cs/ww/en/view/109794377)
- Compatibility of Microsoft updates, Online Support under entry ID 18490004 (https://support.industry.siemens.com/cs/ww/en/view/18490004)

3.3.1 Operating system

Information regarding the release of SIMATIC products with various operating systems (32-bit and 64-bit) is included in:

- SIMATIC PCS 7 Product Catalog (https://support.industry.siemens.com/cs/de/en/view/109745632)
- Compatibility tool (www.siemens.com/kompatool)
- Online help, readme file

The security updates provided by Microsoft and "Important Updates" for the Windows operating system are tested by Siemens for compatibility with SIMATIC software and released, see note under chapter "Updating the system software (Page 170)".

3.3.2 Basic software for user administration

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

- Definition of user groups with various authorization levels for operation and maintenance
- Definition of users and assignment to user groups
- Determination of adjusted plant structure and drive storage including authorizations

Access to the SIMATIC PCS 7 system components is controlled by SIMATIC Logon. You can find additional information on installing and configuring the various SIMATIC Logon components in Chapter "Setting up user administration (Page 41)" and in SIMATIC Logon configuration manual.

3.3.3 Software components for engineering

Some of the most important functions of the SIMATIC PCS 7 engineering software are described below.

See also

- Manual "PCS 7 Engineering System", chapter 8.7, Online Support under entry ID 109800500 (https://support.industry.siemens.com/cs/ww/en/view/109800500)

Multiproject engineering

For a description of setting up and using multiprojects, see chapter "Project setup (Page 57)" of this manual.

Process Control Libraries

The process control libraries contain ready-made, tested objects (blocks, faceplates, and symbols). When these libraries are used, engineering is usually limited to the configuration of the relevant objects. One major advantage of using predefined objects when engineering automated systems is the lower-level software categorization (see chapter "Software categorization according to GAMP 5 Guide (Page 138)") and the possibility of implementing updates. Therefore, the validation work required is less than that for user-specific blocks.

WinCC Configuration Studio

The WinCC Configuration Studio provides a simple means of configuring bulk data for OS projects. The user interface is split into a navigation area and a data area oriented on Microsoft Excel.

The WinCC Configuration Studio includes the following editors and functions:

- Tag Management
- Alarm Logging
- Tag Logging
- User Archive
- User Administrator

CFC (Continuous Function Chart)

The CFC Editor provides a graphic interface for configuring automation and control functions. Drag & drop is used to move function blocks from libraries to a CFC, where they are interconnected and configured in accordance with requirements.

SFC (Sequential Function Chart)

The SFC Editor facilitates the graphic configuration and commissioning of sequential controls. Essential components here are steps and transitions, as well as simultaneous and alternative branches.

Import/Export Assistant (IEA)

The Import/Export Assistant is a tool used to configure systems which feature recurring functions and/or plant units. Process tag lists or CAD charts previously created in the planning phase are used during configuration to create CFCs for process tags, for the most part automatically. During this process, replicas of the models are generated and then supplied with specific data, see chapter "Bulk engineering (Page 87)".

Plant Automation Accelerator (PAA)

PAA enables optimized bulk engineering using object orientation and its integrated type-instance concept for SIMATIC PCS 7. This minimizes the risk of errors. Control module types (CMTs) are used to create templates from which instances are generated. The instances are linked to the template and can be updated when a change is made to the template.

Additional information regarding configuration and the advantages of using the PAA can be found in chapter "Type/instance concept with the PAA (Page 89)".

Block protection

Blocks can be protected from changes and access so that only the inputs and outputs are still accessible. "S7 Block Privacy" (PCS 7 V8.0 and higher) provides greater security than the previous Know-How protection and should therefore be used preferentially for sensitive areas in particular, see chapter "Write protection for CFCs/SFCs and SFC types (Page 153)" on write protection and chapter "Block encryption with "S7 Block Privacy" (Page 155)" on block encryption.

Note

In order to work with blocks encrypted with "S7 Block Privacy", the AS must have a CPU 4xx with firmware version V6.0 or higher.

Version Trail

SIMATIC PCS 7 Version Trail enables multiprojects, single projects, and project-specific libraries to be backed up together with the assignment of unique version ID for the archived projects.

It is possible to back up multiprojects, projects, and libraries at defined times automatically and with versioning, and to read back block parameters in a time-controlled manner.

For more information on configuration and use of "Version Trail", refer to chapter "Versioning of projects with Version Trail (Page 147)".

SIMATIC BATCH

SIMATIC BATCH is a SIMATIC PCS 7 program package that enables discontinuous processes, known as batch processes, to be planned, controlled and recorded. It can be operated as a single user station system or a client/server system and can be used in various different plants, thanks to its modular architecture and scalability. SIMATIC BATCH servers can be configured redundantly.

In principle, the functions of SIMATIC BATCH can be divided into four areas:

- Recipe system: Creation and management of master recipes and library operations
- Batch planning: Planning and rescheduling of batches and production orders
- Batch control: Operation and visualization of the batches released for production or the associated control recipes, including visualization of the current unit allocation
- Batch data management: Collection, storage and reporting of batch data

The chapter "Recipe creation with SIMATIC BATCH (Page 97)" for additional information on configuration and use of SIMATIC BATCH.

Route Control

The SIMATIC Route Control additional software package is used to configure, monitor, and diagnose materials handling (paths) within a plant. It is fully integrated in SIMATIC PCS 7 and SIMATIC BATCH.

For more information on configuration and use of "SIMATIC Route Control", refer to chapter "SIMATIC Route Control (Page 104)".

Simulation with S7-PLCSIM

S7-PLCSIM is a simulation tool for S7 user programs. This software component, which is available as an option, simulates a SIMATIC S7-CPU on a programming device or PC. The configured application software can be tested without the use of AS hardware (CPU and/or signal modules). Up to 8 CPU instances can be simulated.

Communications processors and Route Control cannot be simulated.

Note

The use of S7-PLCSIM is of particular interest for the test system, for example, for typical tests.

For a subsequent operation with an Ethernet network, the Ethernet connection should be configured beforehand in PLCSIM, since all communication links have to be reconfigured for the use of MPI.

Simulation with SIMIT and Virtual Controller

SIMIT can be used from the simulation of the field level through to process simulation, see chapter "Simulation for test mode (Page 145)".

3.3.4 Software components for operation level

Basic software for Operator System (OS)

Systems for the operator control and monitoring of the plant are implemented either as single or multiple station systems.

With a single station system, all operator control and monitoring tasks can be handled on one PC.

A multiple station system (client-server architecture) consists of operator stations (OS clients) and one or more OS servers, which supply the OS clients with data.

Redundant systems can be set up to increase availability.

Note

The number of licenses for the operator stations can be increased at a later time using suitable packs. When extending/updating a license, the existing license must be available, i.e. runtime cannot be active. Online extension is only possible for redundant servers.

SIMATIC BATCH and Route Control

SIMATIC BATCH and SIMATIC Route Control each have their own operating components. Some functions are also integrated in the basic OS, however, and can be operated from there.

SFC Visualization additional software

An SFC (sequential function chart) is used as a sequential control system (also known as a sequencer) of processes. SFCs consist of a sequence of steps that are separated from one another in each case by step enabling conditions (or transitions). These step-enabling conditions can take the form of simple comparisons or complex logic (SFC calculations).

Using SFC Visualization, the configured SFCs can be displayed on the operator station and operated in manual mode. SFC Visualization enables processes to be clearly displayed by showing their different process actions.

No additional effort is necessary to configure the SFC visualization.

OS Web Option additional software

The PCS 7 OS Web Option enables the PCS 7 plant to be operator controlled and monitored via the intranet or internet.

As of SIMATIC PCS 7 V9.0, SIMATIC BATCH OS control elements (SIMATIC BATCH OS Controls) can also be displayed with the OS Web Option.

Note

Use of the Web option in a controlled environment must be thoroughly discussed and agreed with the customer. Aspects such as access to the Web Client, critical or non-critical operator control and monitoring functions, logons, and audit trails, as well as a secure data connection, must be considered during these discussions.

Additional information on the use and configuration of the Web option can be found in chapter "PCS 7 Web Option for OS (Page 93)".

3.3.5 Long-term archiving

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

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

Long-term archiving of process values and messages can be set up using an import/export of archives or with the SIMATIC Process Historian option. Both concepts are introduced below.

OS archiving

Process values and messages are stored in a short-term archive based on Microsoft SQL server technology. The data saved on the archive server can be exported to another computer and, if required, read back or permanently transferred to a long-term archive, see chapter "Setting up process value archives (Page 128)".

SIMATIC Process Historian

A SIMATIC Process Historian can be used to centrally acquire and archive process values and messages from several SIMATIC PCS 7 OS servers (also redundant systems) as well as batch data. Transparent access to the archived data for viewing the messages and process values in the user interface is handled by the system automatically in the background. The messages saved in WinCC archives are fully transferred to the Process Historian. Only those variables that are labeled as being "long-term relevant" are transferred.

If the Process Historian is unobtainable, the completed archives remain on the OS servers and are transferred later when the link to the Process Historian is reactivated. For this purpose, sufficient memory volume is to be planned on OS servers. Monitoring of the network connection may also be advisable.

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

See also

- Manual "PCS 7 Compendium Part A", chapter 10.4.4 "Long-term archiving", Online Support under entry ID 109809015 (https://support.industry.siemens.com/cs/ww/en/view/109809015)
- Manual "Process Historian 2020", Online Support under entry ID 109809287 (https://support.industry.siemens.com/cs/ww/en/view/109809287)

3.3.6 Reporting

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

See also

- Manual "PCS 7 Engineering System", chapter 4.3.5, Online Support under entry ID 109800500 (https://support.industry.siemens.com/cs/ww/en/view/109800500)

Report Designer

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

The Report Designer is also used for documentation of the configured OS project. For this purpose, pre-configured report layouts and print jobs are included in the SIMATIC PCS 7 scope of supply. Both pre-configured report layouts and print jobs can be opened in the Report Designer and modified as required.

Information Server

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

See also

- Manual "PCS 7 Compendium Part A", chapter 10.4.4.1 and 10.4.4.3 "Information Server", Online Support under entry ID 109809015 (https://support.industry.siemens.com/cs/ww/en/view/109809015)

Data exchange via Open PCS 7

Open PCS 7 can be used to exchange data with external systems, such as the plant management and production control level, MES level, or ERP level via the OPC interface, without knowledge of the SIMATIC PCS 7 project topology being required. OPC (Open Platform Communications) refers to a uniform, vendor-independent software interface, the standard of which was defined by the OPC Foundation. The OPC Foundation is an alliance of leading companies in the field of industrial automation.

Information on OPC is available on the internet (https://opcfoundation.org/). The use of Open PCS 7 is described in more detail in chapter "Open PCS 7 (Page 96)".

3.4 Application software specification

In addition to the selection and definition of the hardware (see chapter "Selection and specification of the hardware (Page 26)") and the standard software components used (see chapter "Specification of the basic software (Page 29)“), the specification of the application software is an essential part of the entire specification. Along with the function specification, the specifications for system configuration and design of the system serve later as acceptance criteria during system verification (FAT, SAT, etc.).

The specification of configuration and design can consist of only one document, but usually consists of multiple documents. Additional, separate documents are often added as supplements, e.g. process tag list, I/O list, parameter list, P&ID, etc. Like for the other specification documents, the status of these documents (version, approval) must be clearly defined.

See also

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

In addition to the previously mentioned hardware specification, the specification can be divided as follows, for example:

Configuration and design (general)

- Organization of domain, domain administration, workgroup
- User administration in Windows,
  Definition of user groups, users, authorizations, local users, configuration of SIMATIC Logon, WinCC user administration, SIMATIC BATCH permission management, Route Control user groups, etc.
- Domain and PC profile
- Printer configuration
- Archive configuration (archives, archive cycles, batch reports)
- Interfaces (S7 connections, OPC, discrete I/O processing)

HMI specification

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

- Screen layout and navigation
- Plant pictures, unit pictures, detail pictures of interfaces
- Operator level, access authorizations, if any
- Picture hierarchy
- Screen resolution, picture cycles
- Block icons, faceplates used
- Message capability, message classes, priorities, representation, see chapter "Specification (Page 106)"

Software design specification

- General information such as name of multiproject, name of projects, name of libraries, plant hierarchy
- Appropriate subdivision of plant and plant unit areas for the automation systems, see also chapter "Hardware specification (Page 26)"
- Software structure, typical and module specification, possibly in a separate document
- Control modules (CM) and control module types (CMT) (states, behavior, response to restart)
- Equipment modules (EM) and types (EMT) (states, logic status, behavior, configuration)
- Route Control, if present (function, interface blocks)
- SIMATIC BATCH (function, distribution of recipes, use of forms)
- Any other utilized functionalities, such as RFID etc.
- Power failure and restart behavior (behavior of PC stations and automation systems, failure of an AS)
- Time synchronization, specification of time master and slave

- Description of exceptional states for reliable plant operation
- Emergency-Off response

Note

As a basis for configuring batch control, SIMATIC PCS 7 uses the model of ANSI/ISA-88.01; see also chapter "Conformity with the ISA-88.01 standard (Page 98)".

See also

- Application example for specification of technical functions with SFC types as well as instantiation, Online Support under entry ID 33412955 (https://support.industry.siemens.com/cs/ww/en/view/33412955)

3.5 Additional software SIMATIC PCS 7 Add-ons

The SIMATIC PCS 7 Add-on catalog contains solutions for various areas of application or special branches, such as the process industry. The addresses of the relevant contacts for these add-ons are listed in the catalog.

Note

Priority should be given to add-ons from the latest catalog when implementing functions that go beyond the standard scope of PCS 7. See SIMATIC PCS 7 Add-ons (https://support.industry.siemens.com/cs/ww/en/view/109745636).

3.5.1 versiondog – Version assignment and configuration control

The entire lifecycle of a SIMATIC PCS 7 system can be tracked through the version history with versiondog - from planning through commissioning to continuous optimization during operation. If a new version is created, versiondog automatically determines the changes and makes them transparent to the user.

PCS 7 Smart Compare shows the differences between two versions in the familiar SIMATIC PCS 7 project structure. Differences between two CFCs or SFCs are highlighted in color in a graphic comparison. The audit trail of versiondog allows you verify at any time who made a change, when it was made, what was done and why it was done.

See also

- PCS 7 Add-on description on the Internet (https://mall.industry.siemens.com/mall/en/WW/Catalog/Products/10048340?tree=CatalogTree), including manufacturer details

3.5.2 OPD – User dialogs and electronic signatures

The software operator dialog (OPD) simplifies the interaction between operating personnel and process control system. As a powerful operator tool, it facilitates control of the process and provides complete proof of all manual operations.

The OPD software, which can be executed in a SIMATIC PCS 7 / SIMATIC BATCH system environment, is based on the Microsoft SQL server software. It uses the SIMATIC logon for user verification and electronic signatures.

See also

- PCS 7 Add-on description on the Internet (https://mall.industry.siemens.com/mall/en/de/Catalog/Products/10037427?tree=CatalogTree), including manufacturer details

3.6 Utilities and drivers

3.6.1 Printer drivers

It is advisable to use the printer drivers integrated in the operating system and approved for PCS 7. If external drivers are used, no guarantee of proper system operation can be provided.

3.6.2 Virus scanners

The use of virus scanners in process mode (runtime) is permitted. Additional information on selecting, configuring, and updating virus scanners can be found here:

- Compatibility tool (www.siemens.com/kompatool)
- Manual "PCS 7 Compendium Part F", chapter 9, Online Support under entry ID 109804118 (https://support.industry.siemens.com/cs/ww/en/view/109804118)

When virus scanners are used, the following settings must be observed:

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

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

For more information on the topic of IT Security, see chapter "Information security and data integrity (Page 53)".

3.6.3 Image & partition tools

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

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

See also

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

Note

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

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

3.6.4 SIDSI Backup & Restore Professional

The preconfigured "SIDSI Backup & Restore Professional" system is used for the systematic and secure backup and restoration of virtual machines.

By using the image-based approach to creating backups, you can configure the sources and cycles individually and have them executed automatically.

The following tools are used for backup and restore:

- SIDSI Backup Wizard: Backups of virtual machines to SIVaaS systems and of IPCs with Windows operating system
- SIVaas Back & Restore: Hypervisor operating systems and configuration
- Paragon Hard Disk Manager: Backup & Restore Server (including delivery state)

System Installation and Configuration 4

4.1 Installation of the operating system

When selecting the operating system, observe the information given in chapter "System Specification (Page 25)" and the sources named there.

See also

- Installation instructions for the operating system
- Manual "PCS 7 PC Configuration", Online Support under entry ID 109794377 (https://support.industry.siemens.com/cs/ww/en/view/109794377)

4.2 Installation of SIMATIC PCS 7

To install SIMATIC PCS 7, follow the instructions of the setup program. When required, approved third-party components (e.g. Office) must be installed prior to installing PCS 7. More installation information is contained in the

- Manual "PCS 7 Compendium Part A", chapter 4.3.4, Online Support under entry ID 109809015 (https://support.industry.siemens.com/cs/ww/en/view/109809015)
- Manual "Security Concept PCS 7 and WinCC", Online Support under entry ID 109780811 (https://support.industry.siemens.com/cs/ww/en/view/109780811)
- Manual "PCS 7 PC Configuration", Online Support under entry ID 109794377 (https://support.industry.siemens.com/cs/ww/en/view/109794377)
- Manual "PCS 7 PC Released Modules", Online Support under entry ID 109800496 (https://support.industry.siemens.com/cs/ww/en/view/109800496)
- PCS 7 installation DVD
- Readme files of the individual SIMATIC components

Note

SIMATIC Logon must be selected in the installation setup.

4.3 Setting up user administration

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

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

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

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

Note

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

The individual operating permissions of the software modules are defined in the module description.

All authorization levels for operation via the visualization interface (faceplates, input fields, buttons, etc.) and their assignment to user groups are to be set up according to specifications and tested in the course of the project.

The setup is differentiated in terms of which level the user operates. The membership in certain Windows user groups is therefore required for the start or the configuration of SIMATIC components such as SIMATIC PCS 7 OS or SIMATIC Logon. These user groups are automatically created in the Windows user administration upon installation of the software components and must not be deleted.

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

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

- Setup of user groups and users under on operating systems, see chapter "User administration on the operating system level (Page 42)"
- Setting up security settings in Windows, see chapter "Security settings in Windows (Page 44)"
- SIMATIC user groups, see chapter "SIMATIC user groups (Page 44)"
- Setup and configuration of SIMATIC Logon, see chapter "Configuration of SIMATIC Logon (Page 45)"
- Administration of authorizations for the individual user groups in SIMATIC components (ES, OS, BATCH); see chapter "Administration of user rights (Page 46)"

4.3.1 User administration on the operating system level

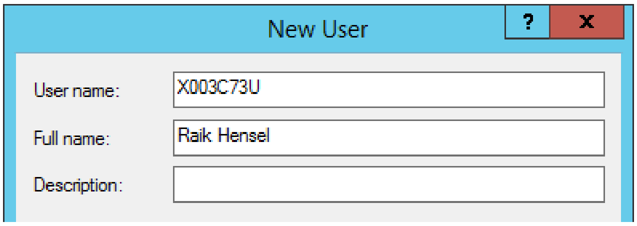
Administration of user permissions using SIMATIC Logon is based on the mechanisms of the Windows operating system. There are two user administration options here:

- Centralized administration in a domain structure
- Administration on a computer of a work group

When using multiple servers or when there are redundant servers, the domain structure must be used to ensure that users will still be able to perform operations and log on even if one domain server fails. The domain server functionality may not be installed on a system with SIMATIC PCS 7 in this case.

Note

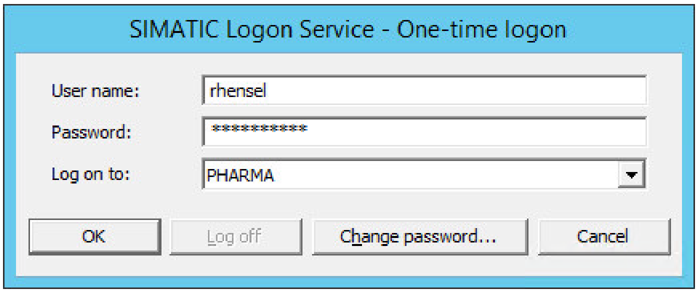
In Windows Computer Administration, the full name must be entered for each user in addition to the user name. This name can be used for the display in SIMATIC PCS 7 after logon to the application and is required for electronic signatures. The full name must therefore be entered.



User name: X003C73U
Full name: Raik Hensel
Description:

See also

- Manual "Security Concept PCS 7 and WinCC", Online Support under entry ID 109780811 (https://support.industry.siemens.com/cs/ww/en/view/109780811)
- Manual "PCS 7 Compendium Part A", chapter 4.2.6 "Workgroup and domain", Online Support under entry ID 109809015 (https://support.industry.siemens.com/cs/ww/en/view/109809015)



User name: rhensel
Password: ***********
Log on to: PHARMA

While a user is authenticated for their operating permissions in the SIMATIC environment when they log on, a "default user" is logged on to the Windows operating system at the same time and has the permissions required for the operating system level. These should not be higher than actually required, see also chapter "Access control to operating system level (Page 51)".

The user logged onto the operating system should be the same user system-wide and should be logged on automatically when an OS computer starts up.

Note

Logons, logoffs and unsuccessful logon attempts can be viewed in the SIMATIC Logon Eventlog Viewer and exported; changes to the user and group configuration are recorded on the operating system level in the Eventlog and can be saved there.

4.3.2 Security settings in Windows

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

When using SIMATIC Logon, the system administrator makes the following security settings in Windows under *Control Panel > Administration > Local security regulations > Security settings > Account regulations / Local regulations*:

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

Note

Following Windows installation, default parameters are set for the password policies, account lockout policies, and audit policies. The settings must be checked and adapted to the requirements of the current project.

See also

- Chapter "Access control to operating system level (Page 51)"
- Chapter "Information security and data integrity (Page 53)"
- Manual "PCS 7 Compendium Part F", chapter 7.4 "Password policies", Online Support under entry ID 109804118 (https://support.industry.siemens.com/cs/ww/en/view/109804118)
- All-round protection with Industrial Security - Plant Security, Online Support under entry ID 50203404 (https://support.industry.siemens.com/cs/ww/en/view/50203404)

4.3.3 SIMATIC user groups

When PCS 7 is installed, local SIMATIC standard user groups are automatically created in the operating system with various rights (SIMATIC HMI, etc.). These must not be changed or deleted.

The defined users and user groups must be made members of these SIMATIC user groups which have the appropriate authorization.

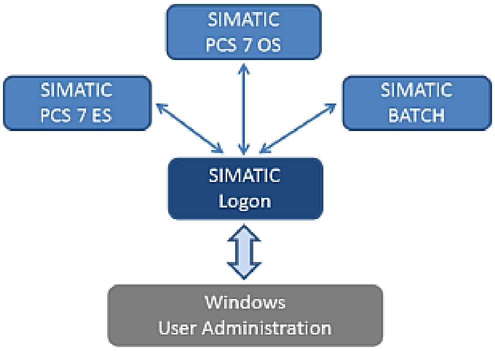
By differentiating between system administrators and users (plant operators) at the Windows level logon, a logical separation is achieved for the computer access authorization.

See also

- Chapter "Access control to operating system level (Page 51)"
- Manual "Security Concept PCS 7 and WinCC", Online Support under entry ID 109780811 (https://support.industry.siemens.com/cs/ww/en/view/109780811)

4.3.4 Configuration of SIMATIC Logon

SIMATIC Logon serves as an interface between the Windows user administration and SIMATIC components. It checks the correctness of logon data for a user against the central user administration. If the logon is valid, the associated user groups are returned to the operator station.



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

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

Note

Events, such as successful and failed logons and logoffs, password changes, etc. are stored in the EventLog database of SIMATIC Logon. This must be taken into account when backing up data, see also chapter "Audit trail and change control (Page 113)".

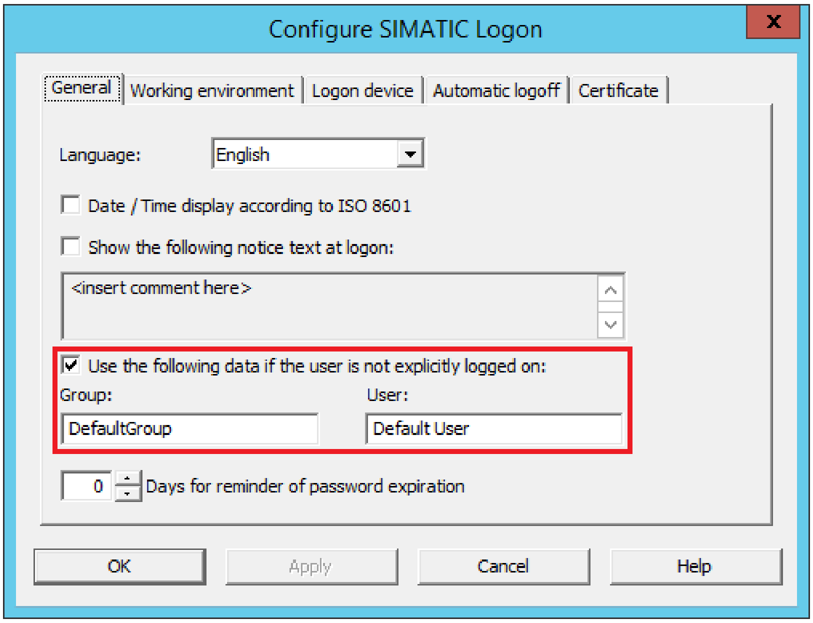
See also

- Manual "SIMATIC Logon", Online Support under entry ID 109804727 (https://support.industry.siemens.com/cs/ww/en/view/109804727)

Default user after user logs off

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

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



Language: English

□ Date / Time display according to ISO 8601

□ Show the following notice text at logon:

<insert comment here>

☑ Use the following data if the user is not explicitly logged on:

Group: DefaultGroup

User: Default User

0 Days for reminder of password expiration

Automatic logoff (Auto Logoff)

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

Note

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

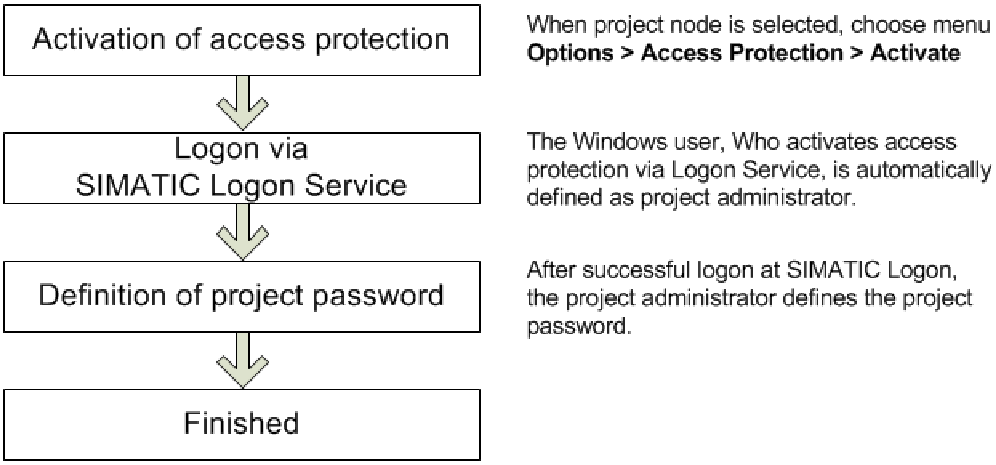
A screen saver should also be disabled when SIMATIC Logon is used. Otherwise, when unlocking the screen, the system would ask for the password of the Windows user, which the PCS 7 OS operator should not know.

4.4 Administration of user rights

4.4.1 Permission management on the Engineering System (ES)

Access to projects and libraries can be controlled using SIMATIC Logon. When access protection is activated for new or unprotected projects, the Windows user who is logged on is automatically defined as the project administrator. That user can then define other users as project editors or project administrators.

To complete activation of access protection, the user must specify a project password which should only be known to the project administrators.


Activation of access protection
Logon via SIMATIC Logon Service
Definition of project password
Finished
When project node is selected, choose menu **Options > Access Protection > Activate**
The Windows user, Who activates access protection via Logon Service, is automatically defined as project administrator.
After successful logon at SIMATIC Logon, the project administrator defines the project password.

"SIMATIC Logon Role Management" serves as the interface for assigning users to the group of project editors or project administrators.

Note

Access protection must be activated for every project and every library used in the multiproject.

Synchronization: Within a multiproject, access protection for one project or library can be passed down to all other projects/libraries.

Possible user permissions on the ES

A user on the ES may be given the following permissions:

Project editor

- Make project changes
- Display change log

Project administrator

- Make project changes
- Display change log
- Enable and disable the change log
- Manage access protection
- Deactivating access protection
- Synchronizing access protection in the multiproject

Note

In order for a user to be assigned to permission roles, they must already be known in Windows administration.

The following presents three possible scenarios for establishing and using protected projects / libraries.

Scenario 1

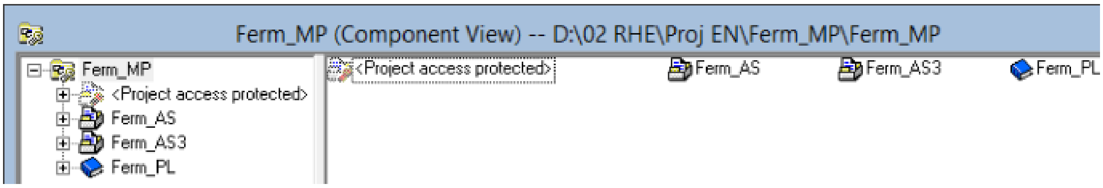
- SIMATIC Logon installed
- User known in Windows
- Access permission for the project is available

When the user has the required permission, they can open a project without any further authentication, provided it is in the same network as the user. This also applies if the project has been taken out of the multiproject.

Scenario 2

- SIMATIC Logon installed
- User known in Windows
- Access permission for the project is not available

If a user does not have access permission, protected projects/libraries are displayed in gray.


Ferm_MP (Component View) -- D:\02 RHE\Proj EN\Ferm_MP\Ferm_MP
Ferm_MP
<Project access protected>
Ferm_AS
Ferm_AS3
Ferm_PL
<Project access protected>
Ferm_AS
Ferm_AS3
Ferm_PL

If the user attempts to open the project, they will be prompted to enter the project password. If the user knows this password and enters it, they are automatically defined as a project administrator.

Note

The project password should only be known to the project administrator.

Scenario 3

- SIMATIC Logon not installed

If SIMATIC Logon is not installed, there is no project administration function. Each time a protected project/library is opened, the project password must be entered. Also in this case, the project password should only be made known to the relevant group of people. If the protected project has been provided by a customer, they must decide whether or not the existing password should be changed in their system.

Note

The way in which the project password is used and the time at which access protection is to be activated on the ES level should be given careful consideration and defined at an early stage.

See also

- Manual "PCS 7 Engineering System", Online Support under entry ID 109800500 (https://support.industry.siemens.com/cs/ww/en/view/109800500)

Note

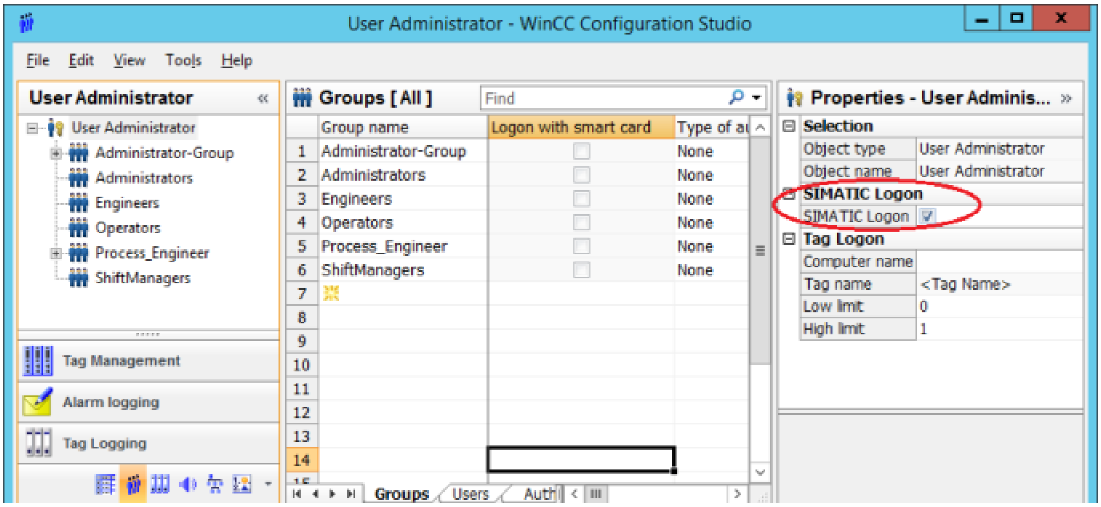
In addition to the scenarios described above, a password can be assigned for accessing the CPU. With a newly configured CPU, the "Read/write protection" option is enabled by default in the "Protection" tab of the CPU object properties as of V9.1 SP1 and higher. Assign a password or change the protection level in this case.

4.4.2 Permission management on the Operator System (OS)

Windows user groups are assigned to PCS 7 OS groups by virtue of their same names. For example, if you want to assign an "Operator" Windows group, an identically named "Operator" group must be created in the PCS 7 OS User Administrator and the required rights assigned. The following procedure must be followed for this:

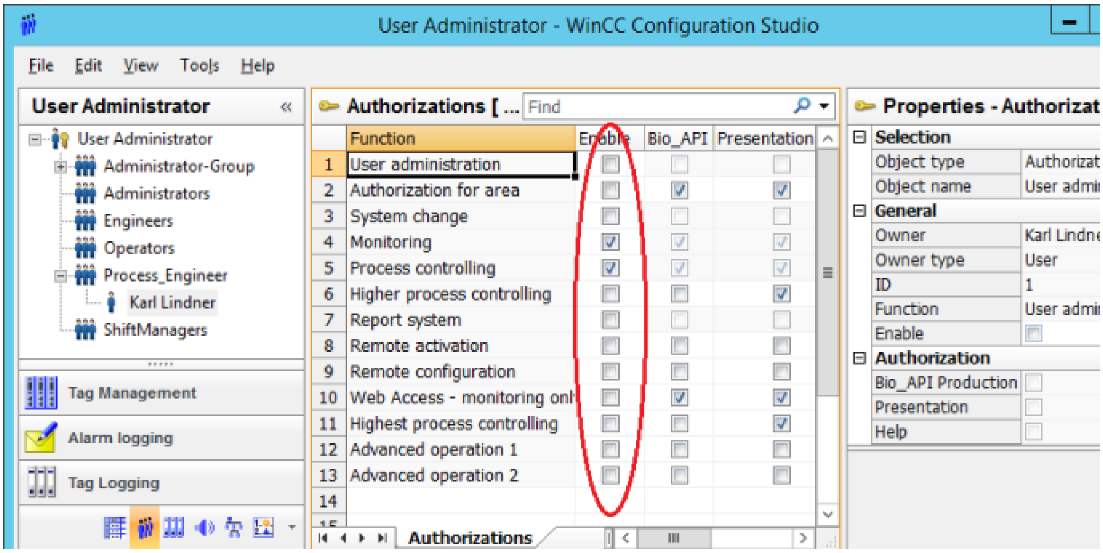
- Open PCS 7 OS project
- Open User Administrator via WinCC Control Center
- Create the group(s)
- Assign the permissions for each group

The figure below shows an example of how operating permissions are assigned to individual groups.



	Group name	Logon with smart card	Type of au
1	Administrator-Group	□	None
2	Administrators	□	None
3	Engineers	□	None
4	Operators	□	None
5	Process_Engineer	□	None
6	ShiftManagers	□	None
7			
8			
9			
10			
11			
12			
13			
14			

Selection	
Object type	User Administrator
Object name	User Administrator
SIMATIC Logon	
SIMATIC Logon	☑
Tag Logon	
Computer name	
Tag name	<Tag Name>
Low limit	0
High limit	1



	Function	Enable	Bio_API	Presentation
1	User administration	□	□	□
2	Authorization for area	□	☑	☑
3	System change	□	□	□
4	Monitoring	☑	☑	☑
5	Process controlling	☑	☑	☑
6	Higher process controlling	□	□	☑
7	Report system	□	□	□
8	Remote activation	□	□	□
9	Remote configuration	□	□	□
10	Web Access - monitoring onl	□	☑	☑
11	Highest process controlling	□	□	☑
12	Advanced operation 1	□	□	□
13	Advanced operation 2	□	□	□
14				

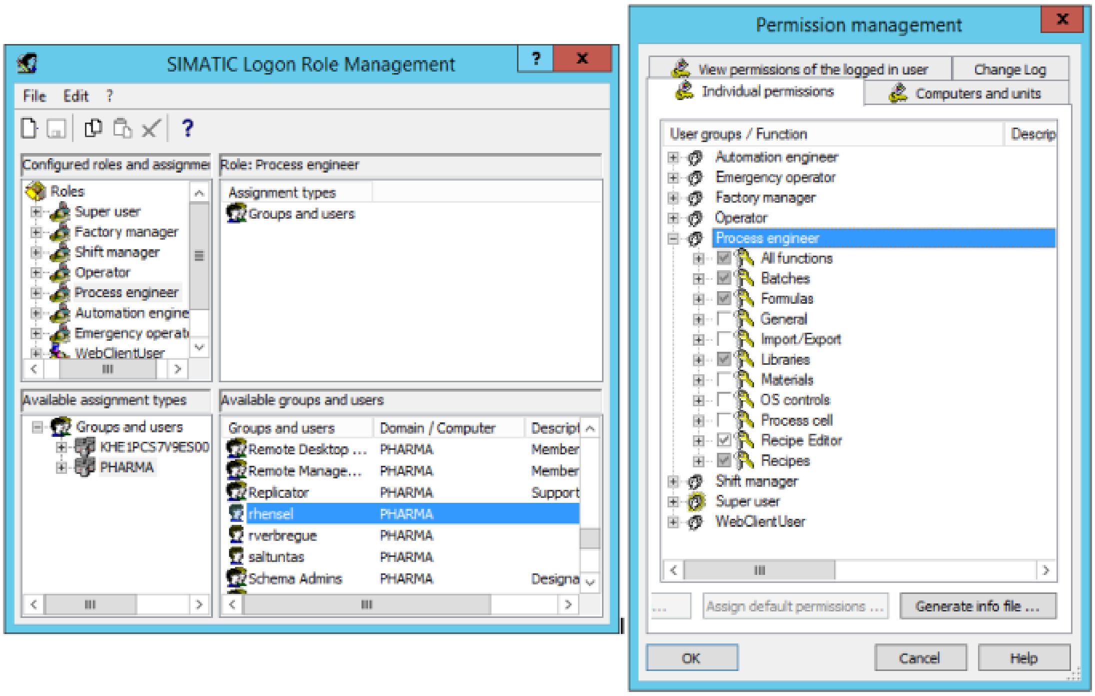
Selection	
Object type	Authorizat
Object name	User admi
General	
Owner	Karl Lindne
Owner type	User
ID	1
Function	User admi
Enable	□
Authorization	
Bio_API Production	□
Presentation	□
Help	□

Note

Centralized management of users, such as that provided by SIMATIC Logon, is essential in many situations, especially in regulated environments. For this, the check mark for activation of SIMATIC Logon must be set in the PCS 7 OS "User Administration" of the respective PCS 7 OS computer.

4.4.3 Permission management in SIMATIC BATCH

Permissions and roles are assigned in the SIMATIC BATCH application using "SIMATIC Logon Role Management".



Groups and users	Domain / Computer	Descript
Remote Desktop ...	PHARMA	Member
Remote Manage...	PHARMA	Member
Replicator	PHARMA	Support
rhensel	PHARMA	
rverbregue	PHARMA	
saltuntas	PHARMA	
Schema Admins	PHARMA	Designa

Process engineer:
- ☑ All functions
- ☑ Batches
- ☑ Formulas
- ☐ General
- ☐ Import/Export
- ☑ Libraries
- ☐ Materials
- ☐ OS controls
- ☐ Process cell
- ☑ Recipe Editor
- ☑ Recipes

The individual roles are assigned to operating permissions in SIMATIC BATCH. The following can also be defined:

- User permissions for a user role
- Permitted user roles per computer
- Permitted user roles per unit

4.5 Access control to operating system level

For the general network configuration, refer to the manuals "PCS 7 Engineering System Configuration" and "PCS 7 and WinCC Security Concept".

Since access to the Windows operating system level should be avoided for security reasons, additional configuration settings are necessary. These settings prevent unauthorized access from SIMATIC PCS 7 process mode to sensitive operating system data.

Note

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

Automatic startup and logon

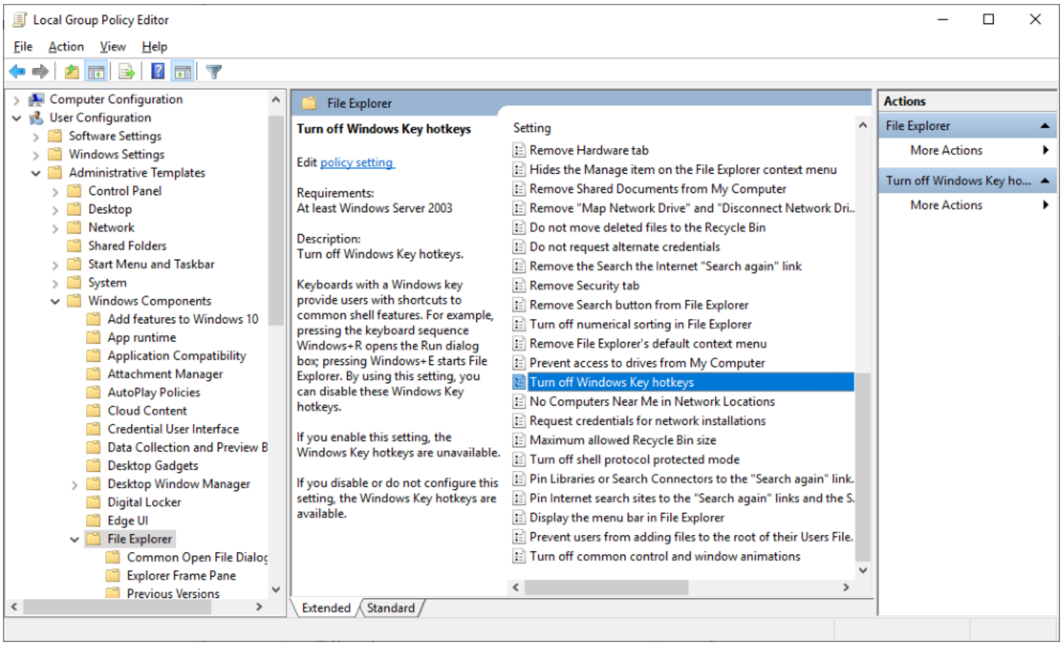
The "default user" on the operating system level should be logged on automatically when each server or client starts up.

Activating the operator control level (runtime)

Automatic starting of the SIMATIC PCS 7 operator control level (OS Runtime) must be activated so that the operating system level cannot be accessed.

4.5.1 Configuration settings in Windows

You can use hot keys (keyboard shortcuts) to go to the operating system level. This option must be disabled for operator stations in particular. This setting is made via the computer policies.



Turn off Windows Key hotkeys

Edit policy setting

Requirements:
At least Windows Server 2003

Description:
Turn off Windows Key hotkeys.

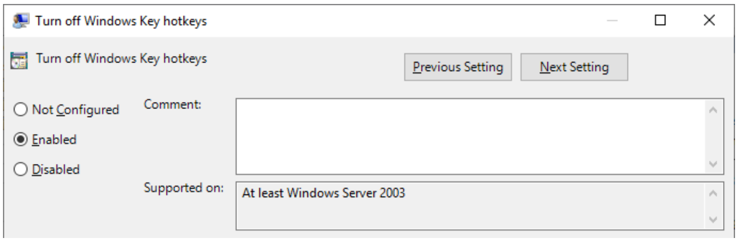
Keyboards with a Windows key provide users with shortcuts to common shell features. For example, pressing the keyboard sequence Windows+R opens the Run dialog box; pressing Windows+E starts File Explorer. By using this setting, you can disable these Windows Key hotkeys.

If you enable this setting, the Windows Key hotkeys are unavailable.

If you disable or do not configure this setting, the Windows Key hotkeys are available.

Setting
- Remove Hardware tab
- Hides the Manage item on the File Explorer context menu
- Remove Shared Documents from My Computer
- Remove "Map Network Drive" and "Disconnect Network Dri..
- Do not move deleted files to the Recycle Bin
- Do not request alternate credentials
- Remove the Search the Internet "Search again" link
- Remove Security tab
- Remove Search button from File Explorer
- Turn off numerical sorting in File Explorer
- Remove File Explorer's default context menu
- Prevent access to drives from My Computer
- Turn off Windows Key hotkeys
- No Computers Near Me in Network Locations
- Request credentials for network installations
- Maximum allowed Recycle Bin size
- Turn off shell protocol protected mode
- Pin Libraries or Search Connectors to the "Search again" link.
- Pin Internet search sites to the "Search again" links and the S.
- Display the menu bar in File Explorer
- Prevent users from adding files to the root of their Users File.
- Turn off common control and window animations

Caution: Disabling the keyboard shortcuts must be enabled for them to be effectively disabled. See the following screenshot.



○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Server 2003

4.5.2 Configuration setting on SIMATIC PCS 7 OS

Access to the operating system during process operation is configured via the OS parameter properties.

It must also be ensured in SIMATIC PCS 7 OS User Administrator that the button for terminating process operation (deactivate OS) can only be clicked if the appropriate permission is available.

4.5.3 Secure configuration

If possible, no OLE objects should be configured, as such objects often allow unauthorized access to folders, files, and programs.

4.6 Information security and data integrity

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

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

Note

Standard passwords stored in the system must be changed specifically for each project. All test accounts must also be deleted at the latest when the system is handed over.

For improved access protection to WinCC databases by deleting standard users, also see the notes in the WinCC Installation Notes in chapter 1.2.2.3, Online Support under entry ID 109792613 (https://support.industry.siemens.com/cs/ww/en/view/109792613).

Definition of a suitable system structure

- For system structure including user management, see Windows settings in chapters "User administration on the operating system level (Page 42)", "Security settings in Windows (Page 44)" and "SCALANCE S (Page 55)".
- Planning of data storage and of input and output devices
- Secure storage of sensitive data with redundancy and access protection
- Use of virus scanners, see chapter "Virus scanners (Page 39)"
- For defined behavior on startup and when operating the user interface, see chapter "Access control to operating system level (Page 51)"

Organizational measures

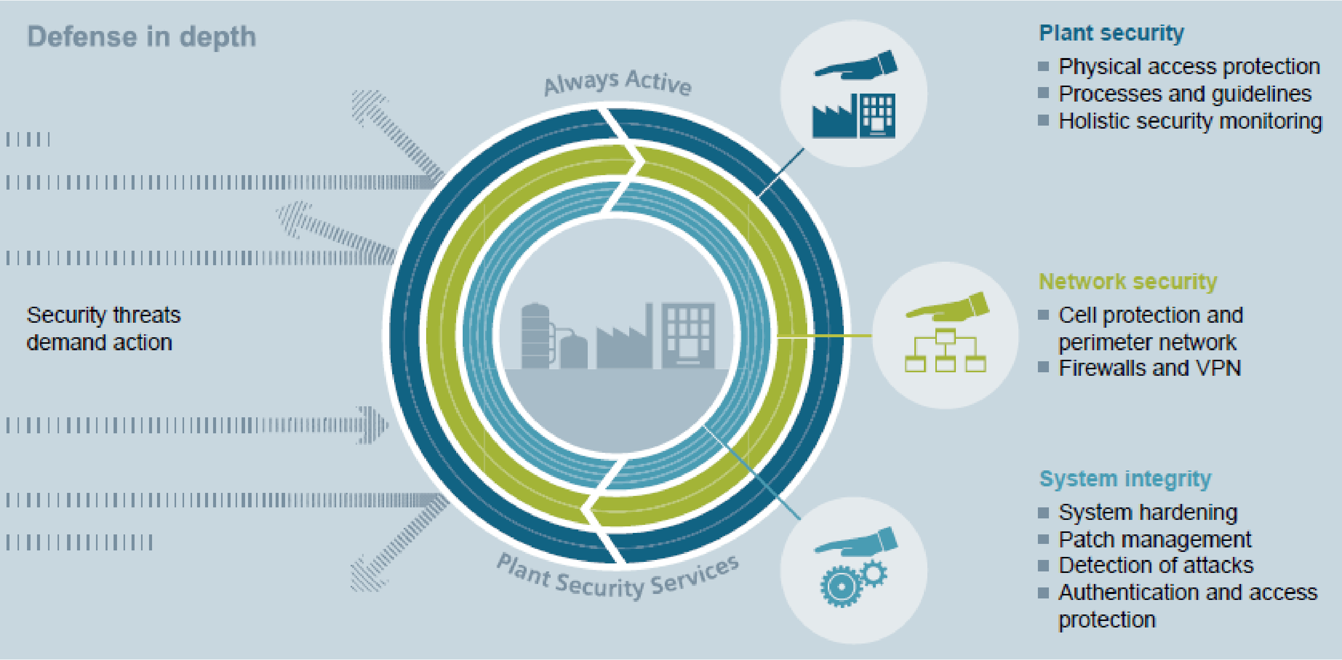
- Planning and assignment of the required access permissions
- Supplementation by codes of behavior, e.g. for handling of USB sticks
- Work instructions for archiving, readback, and possibly data migration

Operating system settings and network security

The settings in the Windows operating system are configured using SIMATIC Security Control, see chapter "SIMATIC Security Control (SSC) (Page 55)".

Defense in depth

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



The experts of Industrial Security Services (https://www.siemens.com/global/en/home/products/services/industry/digital-industry-services/industrial-security-services.html) will gladly support you in designing your security concept.

See also

- Comprehensive information on the topic of "Industrial Security", Online Support under entry ID 50203404 (https://support.industry.siemens.com/cs/ww/en/view/50203404)
- Manual "PCS 7 Compendium Part F – Industrial Security", Online Support under entry ID 109804118 (https://support.industry.siemens.com/cs/ww/en/view/109804118)

4.6.1 SIMATIC Security Control (SSC)

Using SIMATIC Security Control increases the level of computer security. The application can be run either when SIMATIC PCS 7 installation is completed or at a later point in time. The following settings are configured automatically for specific functions (OS client/server, ES, etc.):

- Configuration of the Windows Firewall exception list for SIMATIC PCS 7 communication (firewall can be activated)
- DCOM settings for SIMATIC PCS 7 (Distributed Component Object Model)
- Security-related registry entries

Following installation, the Start > SIMATIC > SimaticSecurityControl menu command can be used to perform configuration at any time. SSC also enables the settings made in the system to be documented.

Note

If the SIMATIC PC station is integrated into another work environment (domain or workgroup), it must be re-configured using SSC.

4.6.2 SCALANCE S

The increasing integration of plant networks in office networks is accompanied by increased security risks, from network problems such as the duplicate assignment of network addresses, to problems with viruses, and even the possibility of attacks by cyber-crime.

In certain applications, the SCALANCE S security modules can be used to counteract these risks. They basically offer two different functions:

Firewall

If a firewall is used, only registered nodes can communicate over the network.

See also

- "Firewall of Industrial Security Appliance SCALANCE S", including attached document, Online Support under entry ID 22376747 (https://support.industry.siemens.com/cs/ww/en/view/22376747)

VPN

A virtual private network (VPN) links external computers in two or more local networks via the internet and encrypts the transferred data at the same time. A VPN connection enables external systems to perform secure remote access over the internet. To do this, SCALANCE S technology uses the widely used IPSec protocol, which provides an extremely high level of security in tunnel mode (VPN tunnel).

See also

- "SIMATIC Net: Configuring VPN tunnel", Online Support under entry ID 109764618 (https://support.industry.siemens.com/cs/ww/en/view/109764618)

Note

SCALANCE S technology offers various applications. Additional information can be found in the manuals of the SCALANCE product series.

Project Settings and Definitions 5

5.1 Project setup

5.1.1 Multiproject

Multiproject engineering allows a project to be divided into several sub-projects so that it can be worked on by more than one person. A higher-level "multiproject", which contains the individual projects (AS, OS, SIMATIC BATCH) and the master data library is defined in the SIMATIC Manager. Projects can be added to and removed from the multiproject. The master data library supports consistent data management within the multiproject.

Note

In a controlled environment in particular, it is required to use the master data library to centrally manage process tag types, control module types (CMT), models, equipment module types (EMT), models, SFC types, and shared declarations.

The SIMATIC PCS 7 "New project" wizard assists you in creating projects. It automatically creates a multiproject. A new project can be added to an existing multiproject as an empty or a pre-configured project. The project name to be assigned must be previously defined in the software specification, as it can be difficult to subsequently rename a project.

For multiproject engineering with SIMATIC BATCH, distributed engineering is only possible when certain conditions are met, see the following entry in the Online Support.

See also

- Manual "PCS 7 Compendium Part A", chapter 5.2 "Required settings in the SIMATIC Manager" and chapter 5.3 "Creating the multiproject", Online Support under entry ID 109809015 (https://support.industry.siemens.com/cs/ww/en/view/109809015)
- "Multiproject engineering with SIMATIC BATCH", Online Support under entry ID 23785345 (https://support.industry.siemens.com/cs/ww/en/view/23785345)

For projects whose size means they are suitable candidates for division into several multiprojects, the project structure and modes of operation must be carefully planned and documented. Your usual Service & Support contacts would be happy to assist you with this.

Note

Good coordination among the project team is essential, especially in larger projects! Therefore, to the extent possible, actions such as archiving, compilation, or downloads should be scheduled so that they do not block the entire team.

5.1.2 Multiproject / multiuser engineering

The configuration of an extensive range of projects can be performed in parallel by various users, whereby the users process different resources.

Multiuser engineering is activated in a property on the PCS 7 OS server. A resource dialog provides an overview of which resource is in process on which computer.

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

Also read the notes in the manual "PCS 7 Engineering System" as well as in the entry listed below in the Online Support.

See also

- Manual "PCS 7 Engineering System", chapter 7.3, Online Support under entry ID 109800500 (https://support.industry.siemens.com/cs/ww/en/view/109800500)
- "PCS 7 Multiproject / Multiuser Engineering", Online Support under entry ID 22258951 (https://support.industry.siemens.com/cs/ww/en/view/22258951)

5.2 Referenced OS stations

Using a "referenced OS station" allows you to create a reference to an existing OS station. Several OS types can be configured as samples and all other OS stations derived from these samples, similar to the way the type/instance concept works.

Note

We do not discuss the assignment of a standard server for the OS client at this time. See chapter "Audit Trail PCS 7 OS (Page 116)".

Configuration types

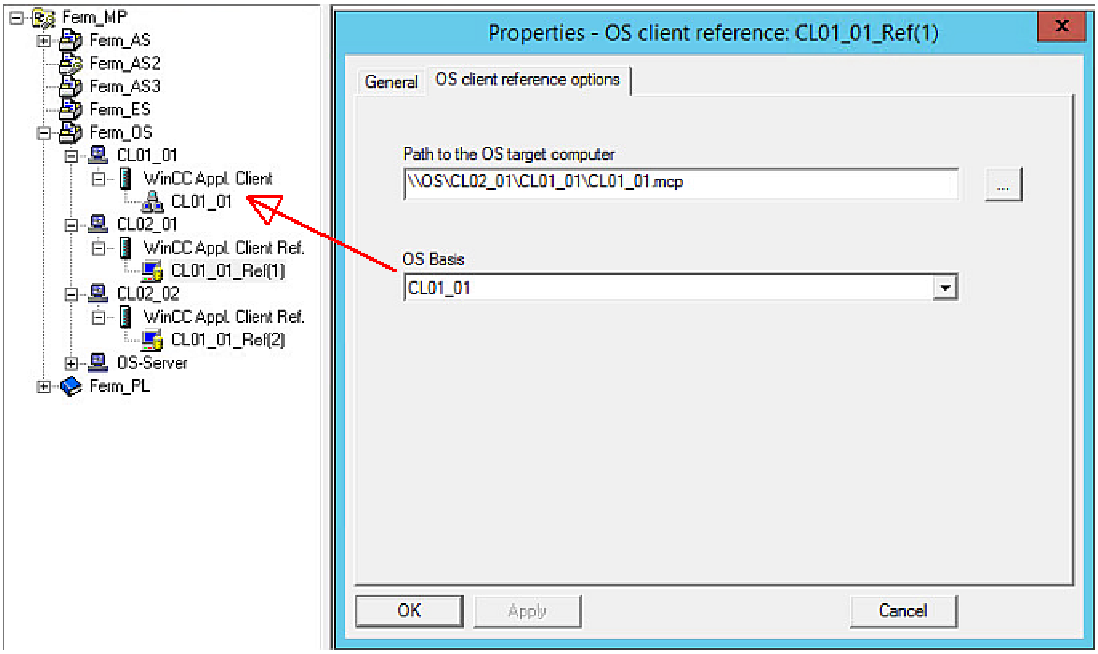
The following types of OS stations can be referenced:

a) Referenced station for OS single user station (WinCC application ref.)

b) Referenced station for OS client station (WinCC application client ref.)

Software configuration using the example of a client

The referenced OS client station needs a standard multiclient as a reference. A referenced OS client station is then added to the project and the “OS Basis" is defined in the object properties (see figure). The number of referenced OS client stations is limited by the maximum number of operator stations, which is defined by SIMATIC PCS 7.



Path to the OS target computer: \\OS\CL02_01\CL01_01\CL01_01.mcp

OS Basis: CL01_01

Note

If the reference station is changed, all OS stations which reference it must be loaded.

Advantages of using referenced stations

Referenced stations help to minimize errors and the amount of work required. The reference station only has to be thoroughly tested in accordance with its specification. For the referenced stations merely special configuration features need to be taken into account, for example, screen resolutions, PCS 7 OS client-specific operating ranges, and user rights. General function tests also need to be performed.

5.3 Using the master data library

To allow several instances of the same functions to be generated, SIMATIC PCS 7 offers a duplication option, based on a defined software procedure. However, this is only possible in conjunction with the master data library, which contains not only the folders for types and models, but also the folders for shared declarations (units, enumerations, and equipment properties) as well as OS pictures and OS reports.

The project typicals are created on the basis of the libraries used (PCS 7 standard library, Advanced Process Library APL, etc.). They are then stored and managed in the master data library. The PCS 7 standard libraries include templates that can be used. Even equipment modules and complete units can be stored in the master data library as templates and be duplicated from there.

Note

The modules and typicals should be verified in a module test and approved by the customer prior to instantiation.

Not only must the same versions of faceplates, SFC types, and typicals be used in all projects within a multiproject, but such projects must also be based on a common plant hierarchy and shared declarations. The individual projects must be synchronized with the master data library for this.

Note

SIMATIC Version Trail can be used to clearly archive and organize versions of the master data library during the course of the project.

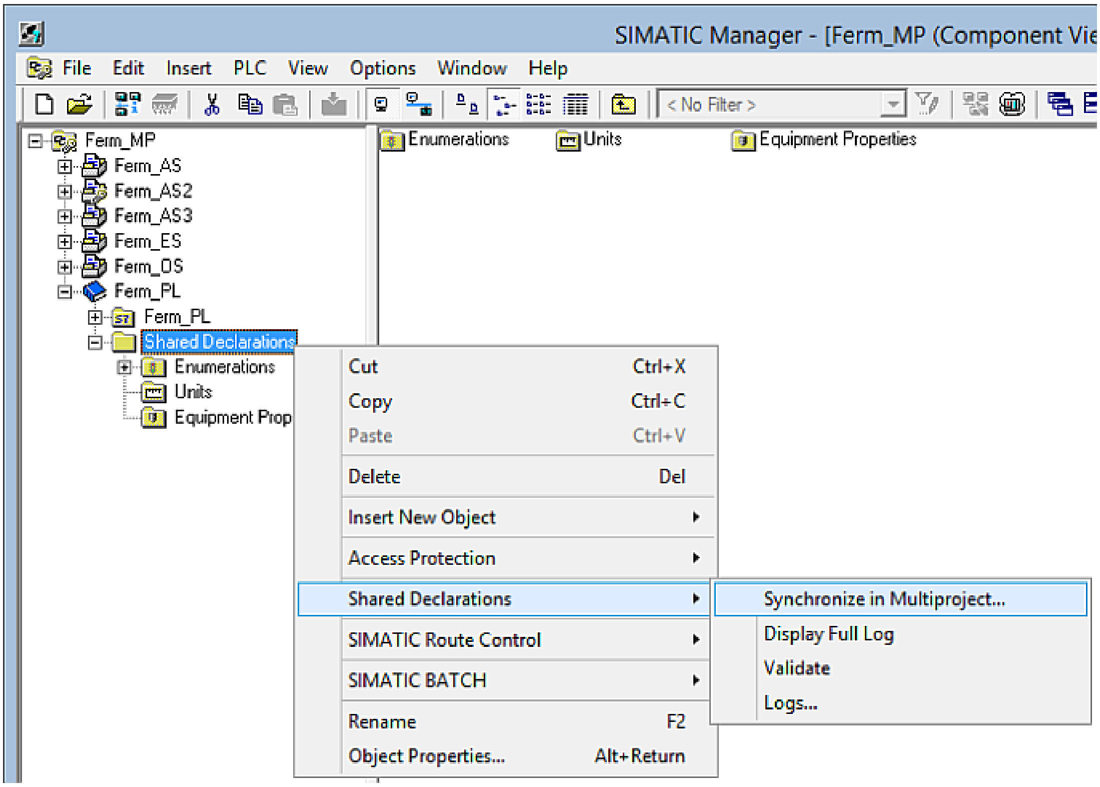
The faceplates, types, and shared declarations are the smallest user software modules. These are first generated and released during configuration before they are duplicated via the IEA interface or manually, see also chapter "Bulk engineering with the IEA (Page 88)" as well as chapter "Type/instance concept with the PAA (Page 89)".

See also

- Manual "PCS 7 Compendium Part A", chapter 8.2.1 "Process tag types" ad 8.2.2 "CMT", Online Support under entry ID 109809015 (https://support.industry.siemens.com/cs/ww/en/view/109809015)

5.3.1 Synchronizing shared declarations

Shared declarations are generated in the master data library automatically when the multiproject is created. These declarations can be synchronized to make them available in all projects. Centralized maintenance in the master data library is strongly recommended in order to ensure consistency throughout the multiproject.

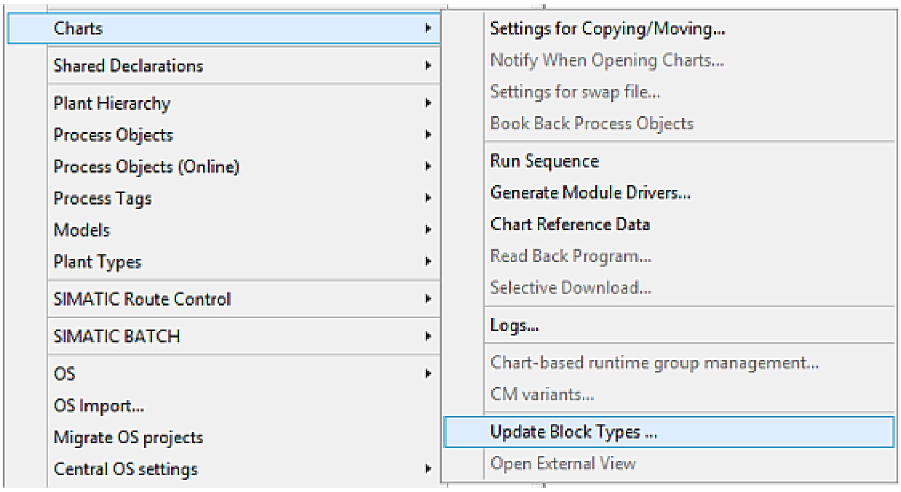


5.3.2 Updating template types

Template types (blocks, CFC, SFC, etc.) must be created and maintained in the master data library in order to achieve data consistency. So that the instances used in the projects correspond to the current template types from the master data library, these can be compared to each other.

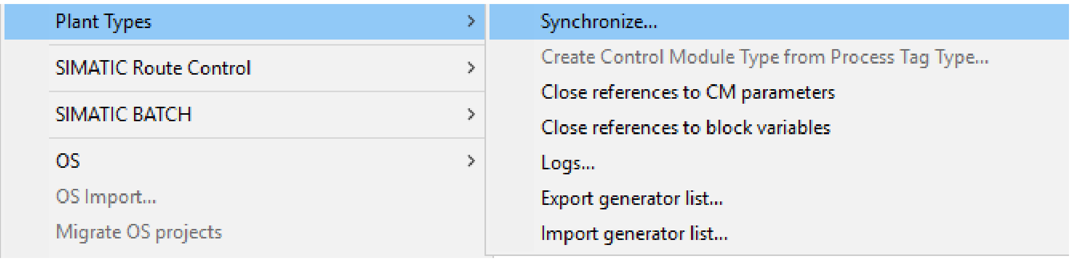
The differences can be checked using a version comparison before the synchronization.

To update the block types and SFC types, select the block folder or a block in the master data library followed by "Options > Charts > Update Block Types...".



For process tag types and models, the "Create/change process tag types" and "Create/change models" wizards are available for the centralized changes to replicas.

You start the synchronization for control module types (CMs or CMTs) via the shortcut menu "Technological Types > Synchronize...". in the plant view of the project.



See also

- Manual "PCS 7 Engineering System", chapter 7.4, Online Support under entry ID 109800500 (https://support.industry.siemens.com/cs/ww/en/view/109800500)
- Manual "PCS 7 Compendium Part A", chapter 8.1.6 "Updating block types", Online Support under entry ID 109809015 (https://support.industry.siemens.com/cs/ww/en/view/109809015)
- Manual "Synchronizing control module type", Online Support under entry ID 109758382 (https://support.industry.siemens.com/cs/ww/en/view/109758382)

5.3.3 Synchronizing the plant hierarchy

Four views are available in SIMATIC PCS 7 for configuration purposes:

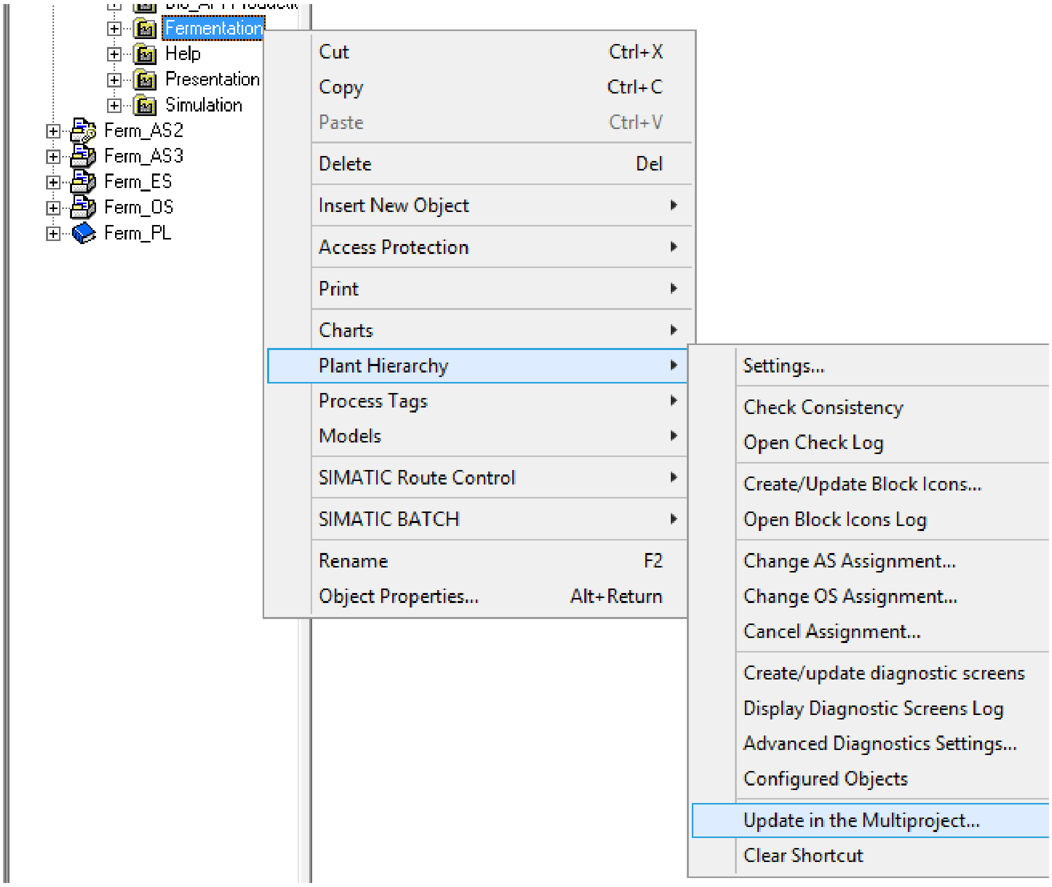
- Component view for configuring hardware
- Plant view for structuring the process engineering hierarchy

- Process object view for centralized editing of parameters, signals, messages, picture objects, archive tags, etc.
- Technological list editor for the engineering of parameters, signals via import/export using Microsoft Excel

It is advisable to structure the plant hierarchy in the same way in all projects within a multiproject. To do this, place the plant hierarchy in a project (recommendation: OS project) and transfer this structure to all projects of the multiproject. The shared declarations of the template project are also transferred to the selected projects as part of this process. This forms a connection between the hierarchy folders.

See also

- Manual "PCS 7 Compendium Part A", chapter 5.6 "Creating the plant hierarchy", Online Support under entry ID 109809015 (https://support.industry.siemens.com/cs/ww/en/view/109809015)



Note

The template project takes on a kind of master role, in other words the names of the created hierarchy folders can only be changed centrally in the template. Names can only be changed in the replicas once this connection has been removed.

5.4 SIMATIC NET

5.4.1 Configuring SIMATIC NET

SIMATIC NET reflects the gateways used in the project. The SIMATIC NET network addresses and settings for the AS, OS, distributed I/O, etc. described in the specification must be used for configuration. This is verified later during testing (for example, FAT, IQ).

The gateways are configured using the "Advanced PC Configuration" procedure. With Windows, all the automation stations (AS) and operator stations (OS) can be configured on a central engineering station and the configuration files can be downloaded.

Specifically, the following connections are configured:

- AS/OS connections
- AS/AS connections
- ES/AS connections
- Remote I/O connections

These connections can also be designed to be fault-tolerant.

Additional information can be found in the SIMATIC NET documentation.

5.4.2 Plant bus and terminal bus

Industrial Ethernet offers a comprehensive range of network components for electrical and optical data transmission. In SIMATIC PCS 7, a distinction is made between a plant bus and a terminal bus. To guarantee a high degree of security and performance, it is advisable to install these two buses separately.

Industrial Ethernet is used as the plant bus. The automation stations are connected to the OS servers and the engineering station over the plant bus.

The PCS 7 servers are connected to the clients, archive servers, and higher-level MES systems over the terminal bus.

See also

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

5.4.3 PROFIBUS

Reliable communication with the field level must be in place in order to ensure trouble-free plant operation. Such communication is based on a high-performance real-time bus system such as PROFIBUS versions DP and PA.

See also

- Manual "SIMATIC NET PROFIBUS Network Manual", Online Support under entry ID 35222591 (https://support.industry.siemens.com/cs/ww/en/view/35222591)
- Manual "PCS 7 Engineering System", chapter 4.6.7, Online Support under entry ID 109800500 (https://support.industry.siemens.com/cs/ww/en/view/109800500)
- Manual "PCS 7 Compendium Part A", chapter 6.4 "Settings for CP 443-5 Ext as PROFIBUS master", Online Support under entry ID 109809015 (https://support.industry.siemens.com/cs/ww/en/view/109809015)

Note

The configuration of the PROFIBUS devices/communication is integrated into the overall project in the SIMATIC Manager. A backup of the engineering project therefore contains the entire user software. This has corresponding advantages in terms of regular data backups and verification of the software within the framework of the test phases.

PROFIBUS DP

Remote I/O stations such as ET 200 can have a simple or a redundant design over electrical or optical PROFIBUS DP networks.

With the help of an isolating transformer (RS 485iS coupler) used as a barrier and the intrinsically safe ET 200iSP, PROFIBUS DP can also be operated in a hazardous area according to the ET 200iSP operating instructions. This makes data transfer rates of up to 1.5 Mbps possible, even in hazardous areas.

Complex process I/O devices such as those listed below can be linked to PCS 7 using predefined add-on blocks:

- SIMOCODE pro motor management system
- MICROMASTER 4 frequency inverters
- SIWAREX weighing system

Also available:

- Function modules (e.g. closed-loop controllers, motor starters, etc.)
- HART modules (for integrating HART field devices)
- F-modules (for fail-safe applications)
- Ex modules (connection of actuators/sensors from EX zone)

HART modules can be configured via PDM, see chapter "SIMATIC PDM (Page 67)".

PROFIBUS PA

PROFIBUS PA can also be implemented in a simple installation or with increased availability. The ring topology can be used here for a redundant structure. The PROFIBUS PA can be run via corresponding devices (Ex-coupler or AFDiS(D)) as well as intrinsically safe bus. As such, devices can be connected from Ex-zones. The AFDiSD is also characterized by its extended diagnostic capability, such as signal level, jitter, etc. according to NAMUR NE107 "Self-Monitoring and Diagnosis of Field Devices" for main cables and spur cables.

See also

- Manual "Bus Links DP/PA Coupler, DP/PA Link and Y Link", Online Support under entry ID 109805389 (https://support.industry.siemens.com/cs/ww/en/view/109805389)

Note

When configured as a diagnostic slave, the FDC 157-0 DP/PA coupler is fully integrated into plant-level PCS 7 Asset Management.

5.4.4 PROFINET

Profinet IO is a manufacturer-independent standard (IEC 61158-5-10) and within the scope of Totally Integrated Automation (TIA), is the joining and extension of the PROFIBUS DP standard, the established fieldbus and Industrial Ethernet. Similarly to PROFIBUS, PROFINET stands for maximum transparency, open IT communication, network security and real-time communication down to the field level.

See also

- Manual "SIMATIC NET / PROFINET", Online Support under entry ID 27069465 (https://support.industry.siemens.com/cs/ww/en/view/27069465)
- Manual "PCS 7 Engineering System", chapter 4.6.8, Online Support under entry ID 109800500 (https://support.industry.siemens.com/cs/ww/en/view/109800500)

PROFINET remote I/O stations such as ET200M can have a simple design over electrical or optical Ethernet networks. In addition to this, there is the option of integrating PROFIBUS DP and PROFIBUS PA devices via a proxy.

PROFINET fulfills the following properties:

- Transmission of time-critical data in guaranteed time intervals.
- Deterministic system: Accurate prediction in terms of the transmission time
- Problem-free communication using other standard protocols within the same network
- Increased availability through media redundancy (MRP)

The following table compares PROFIBUS and PROFINET:

	PROFIBUS	PROFINET
Transmission rate	12 Mbps	100 Mbps
Cycle time	Min. 300 µs	Min. 31.25 µs

	PROFIBUS	PROFINET
Jitter	<1µs	<1µs
User data per device (slave)	244 bytes	64 KB (internal) 8 KB (external)
Number of devices/interfaces	125	250 internal 128 external
Number of devices/supports	1625 3 onboard IF+10 CPs	768 1 onboard IF+4 CPs
Consistent user data	244 internal 128 external	1440 internal 240 external
I/O address space	8 KB internal 8 KB external	8 KB internal 4 KB external

The advantages of PROFINET for the user are the merging of PROFIBUS and Ethernet into one standardized and flexible overall concept.

5.4.5 SIMATIC PDM

SIMATIC PDM (Process Device Manager) is a software package for the configuration, parameter assignment, commissioning, and maintenance of devices (for example, transducers). Among other things, it enables process values and alarms, as well as device status information, to be monitored easily. In addition, commissioning and maintenance is supported by the LifeList functionality which detects and addresses field devices online at the bus.

The modules and field devices can be provided with write protection by the project administrator. This prevents unintended changes to device parameters after acceptance of the process tags.

Modules and field devices can also be marked with the "Device checked" identifier. This identifier allows you to quickly and easily determine the progress of your work. A date and time is assigned to the setting of write protection and the "Device checked" identifier.

Note

Changes to the field device configuration can be reproduced with the PDM "Change log". This function is disabled by default, and it should be enabled under the PDM project settings.

When PDM server/client functionality is used that provides a system-wide device list via web access, an encrypted SSL connection is strongly recommended. In addition, operator authorizations such as "Write to device" must be limited to what is strictly necessary.

Electronic Device Description (EDD)

The EDD forms the basis for device integration. It is supplied by the device manufacturer, made available via the internet, or included in the device catalogs of EDD applications.

SIMATIC PDM is fully integrated in PCS 7. All devices integrated in a project using EDD can be parameterized, commissioned, and maintained from a central engineering station by means of a single tool.

Note

When selecting the devices, ensure that the EDDs must be integrated into the PDM. PDM is supplied with a library of previously integrated device descriptions. A list of the EDDs integrated in the "SIMATIC PDM Device Library" for the respective version can be obtained in Online Support under entry ID 109748100 (https://support.industry.siemens.com/cs/ww/en/view/109748100).

The integration of EDDs not contained in this library can be costly and in some cases impossible. As a general rule, an integration test is advisable for the field devices prior to the final selection.

Export functions in SIMATIC PDM

SIMATIC PDM provides the option of using an export function to back up data of one or more field devices including the following:

- Device parameters
- Change log, changes sorted according to object
- Calibration report, contains information relating to commissioning and maintenance, as well as test results

Note

Version information can be saved in the device’s comment field. This information is then exported together with the device data. A version can also be identified by the name given to the export file.

As the export file contains a reference to an appropriate transformation file, the content of the export file is displayed in the Web browser in a readable HTML format. The corresponding transformation file ("PDMExportEddl.XSL" for the device parameters and change log or "PDMExportCalibration.XSL" for the calibration report) is copied to the export file location as part of the export procedure.

Note

If the export file is copied to a different directory or computer and the HTML display is to be used, the corresponding transformation file must also be copied.

5.5 OS Project Editor

The OS Project Editor in SIMATIC PCS 7 serves as the basic tool for configuring the user interface, for example, for setting the screen layout, screen resolution, etc.

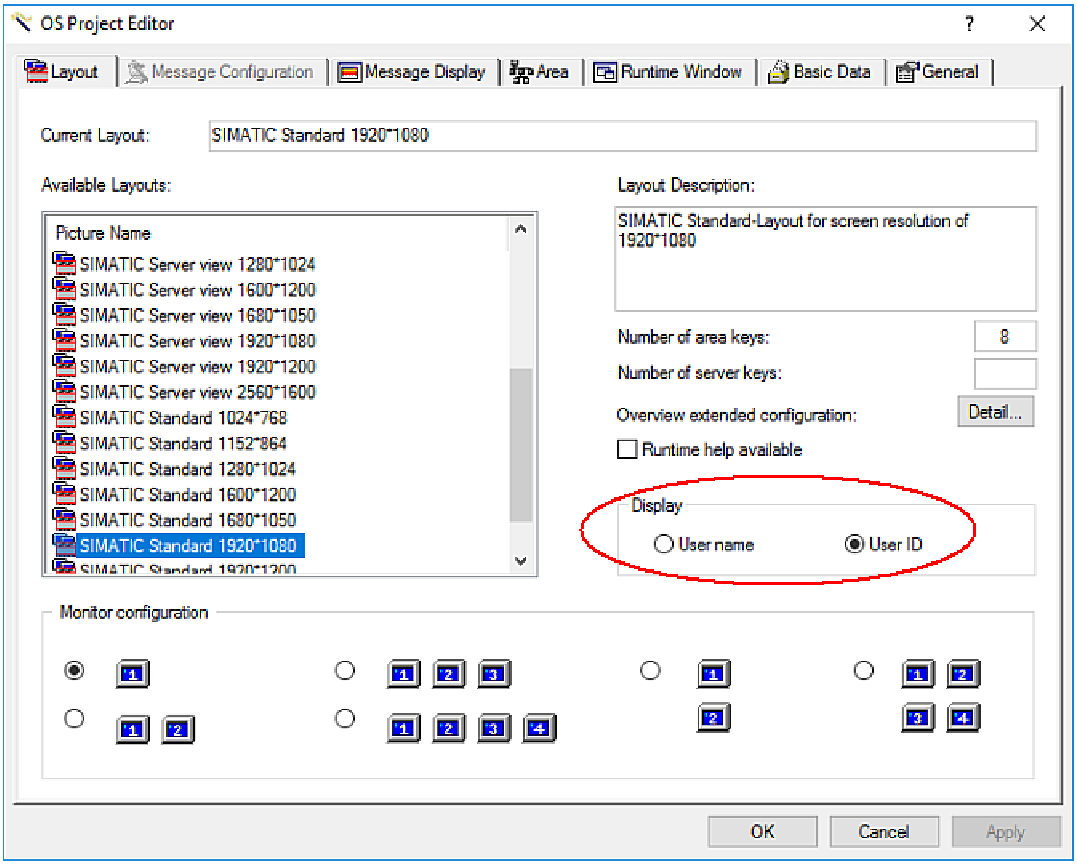
When an OS project is created in the SIMATIC PCS 7 ES, the OS Project Editor is initialized with the default settings.

Many of these default settings can and should be retained in projects. Deviations must be documented and require special attention in every update of the system.

Some settings are always project-specific. These settings and any changes in response to customer requirements are defined in the specification.

See also

- Manual "PCS 7 Operator Station", Online Support under entry ID 109794374 (https://support.industry.siemens.com/cs/ww/en/view/109794374)
- Manual "PCS 7 Compendium Part A", chapter 10.1.4 "Working with the OS project editor", Online Support under entry ID 109809015 (https://support.industry.siemens.com/cs/ww/en/view/109809015)



Current Layout: SIMATIC Standard 1920*1080

Available Layouts:

Picture Name
SIMATIC Server view 1280*1024
SIMATIC Server view 1600*1200
SIMATIC Server view 1680*1050
SIMATIC Server view 1920*1080
SIMATIC Server view 1920*1200
SIMATIC Server view 2560*1600
SIMATIC Standard 1024*768
SIMATIC Standard 1152*864
SIMATIC Standard 1280*1024
SIMATIC Standard 1600*1200
SIMATIC Standard 1680*1050
SIMATIC Standard 1920*1080
SIMATIC Standard 1920*1200

Layout Description: SIMATIC Standard-Layout for screen resolution of 1920*1080

Number of area keys: 8

Number of server keys:

Overview extended configuration:

□ Runtime help available

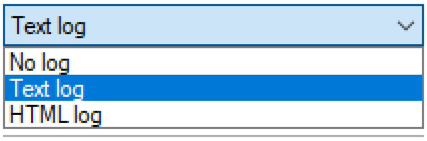
Display: ○ User name ● User ID

Monitor configuration: ● ○ ○ ○ ○ ○

The screenshot above shows the layout of the OS Project Editor. It is also used to specify, for example, whether the user interface should display the "user name" or the "user ID".

- The layout is configured in runtime in the "Layout" tab. This includes the screen formats, number of monitors per OS station and the display of the user name or user ID in runtime.
- Message classes, message types, message blocks, and the PCS 7 standard messages are configured in the "Message configuration" tab.

- Messaging response is configured in the "Message display" tab. This includes the display of messages in the message pages and the group display, message filters and Smart Alarm Hiding.
- Under "Areas" the representation of area and server keys (for example, process cell, unit, functions, etc.) are configured for the overview area.
- The number and arrangement of picture windows is configured in the "Runtime Window" tab. The pictures (graphics) and faceplates are opened in the picture windows in runtime.
- In the "Basic Data" tab, you can specify which modified files of the project are to be overwritten by factory state files. However, you should always ensure when making this configuration change that runtime operation remains consistent and safe.
- The "General" tab contains settings for the OS Project Editor. To ensure continuous logging of the changes, the "append" option should be selected under "Behavior when log files already exist". The log can be stored in HTML or text file formats.



5.6 Time synchronization

Time synchronization is an important feature in automated systems in the GMP environment. When several automation stations (AS) and/or operator stations (OS) interact, messages, alarms, trends, and audit trail data must be archived with synchronized time stamps.

In SIMATIC PCS 7, the default time transmitted on the buses is always the standardized world time UTC (Universal Time Coordinated).

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

Activating time synchronization in SIMATIC PCS 7 means that an active time master handles the synchronization of all OS servers, operator stations, automation stations, and the engineering station. To ensure synchronized time, all the stations in the system must be synchronized so that messages can be processed in the correct chronological order throughout the plant (archiving of trends, messages, redundancy synchronization of servers).

Time synchronization in a Windows work group

In a workgroup environment, the plant bus can be synchronized via a central plant clock. The OS servers obtain the time from the plant bus; they are configured as "cooperative time masters". If no timer is available, an OS server becomes the active time master. The automation stations obtain the time from a central time master; they are configured as time slaves. The OS clients obtain the time from an OS server; they only receive the time from OS servers whose server data they have also loaded.

Time synchronization in a Windows domain

If the automation system is operated in a Windows domain, the domain controller with the PDC role serves as the time master on the terminal bus. It receives its time from a serially connected central time master. The OS servers receive the time from this domain controller via the terminal bus. The OS clients obtain the time from a selected OS sever. The plant bus and, as a result, the connected automation stations (AS) are also synchronized by this OS server (the first server to enter process mode). The server then becomes the active time master.

When high-precision time stamping is required, the automation stations also have to be synchronized directly by a central time master via the plant bus.

If the plant uses components, such as SIMATIC BATCH servers on which no operator station is installed, these also need to be synchronized. This can be done via an additional DCF77 service (central time master) or GPS service or by means of software over the network or the internet.

Time synchronization for package units

Package units may be integrated in many PCS 7 environments. These package units can obtain their time from the Windows domain through the standardized Network Time Protocol (NTP). It is also possible to send the time from one Siemens automation system to another via the S7 protocol.

Note

It must be ensured that the automatic daylight-saving/standard time adjustment is set correctly in the operating system.

If a central time master is used as the clock and the operator station display will be adjusted for daylight-saving time, the central time master must also be set to adjust for daylight-saving time to ensure that all messages are archived with the correct time stamps. This adjustment must be activated on the operator station in the Control Panel > Date and Time > Time Zone.

See also

- Manual "PCS 7 Time Synchronization", Online Support under entry ID 109794383 (https://support.industry.siemens.com/cs/ww/en/view/109794383)
- Manual "PCS 7 Engineering System", chapter 9.9.5.2 "Setting time synchronization", Online Support under entry ID 109800500 (https://support.industry.siemens.com/cs/ww/en/view/109800500)
- Manual "PCS 7 Operator Station", chapter 13 "Time synchronization", Online Support under entry ID 109794374 (https://support.industry.siemens.com/cs/ww/en/view/109794374)
- Manual "PCS 7 Compendium Part A", chapter 10.1.7 "Time synchronization", Online Support under entry ID 109809015 (https://support.industry.siemens.com/cs/ww/en/view/109809015)
- Manual "Security Concept PCS 7 and WinCC", Online Support under entry ID 109780811 (https://support.industry.siemens.com/cs/ww/en/view/109780811)
- Manual "Industrial Ethernet Security", Online Support under entry ID 109751632 (https://support.industry.siemens.com/cs/ww/en/view/109751632)
- FAQ "Time synchronization with DCF77", Online Support under entry ID 19693801 (https://support.industry.siemens.com/cs/ww/en/view/19693801)

- FAQ "Time synchronization in Windows domains", Online Support under entry ID 16620294 (https://support.industry.siemens.com/cs/ww/en/view/16620294)
- FAQ "Settings for time synchronization", Online Support under entry ID 16622902 (https://support.industry.siemens.com/cs/ww/en/view/16622902)
- FDA Guidance 21 CFR Part 11 – Time Stamps, 2002, withdrawn

5.7 Configuration management

The configuration of a computer system consists of various hardware and software components that may vary in complexity and range from commercially available **standard components** to specially customized **user components**. A clear and complete overview of the current system configuration must always be available. This is achieved by dividing the system into configuration elements, which can be identified by a unique designation and a version number and can be distinguished from the previous version.

Defining configuration elements

In terms of hardware, standard components are usually used, which are defined by and documented with their type designation, version number, etc. If customer-specific hardware is used, more work is required; see chapter "Selection and specification of the hardware (Page 26)" for more information.

Such "standard components" are used at least in part for the software, for example, SIMATIC PCS 7 system software, its libraries and options. Just like the hardware, these are defined and documented with designation, version number, etc.

The application software is configured and programmed on the basis of standard software. It is not possible to give a blanket definition of the individual configuration elements that the user software must be divided into, due to differing customer requirements and system designs.

Versioning of configuration elements

While the version designation of standard software cannot be influenced by the user or configuring engineer, work instructions for issuing of version numbers, change control procedures, and the like must be defined for configuring the application software. All configuration elements must be maintained in a transparent manner right from the start of system's creation.

Note

Chapter "Versioning of software elements (Page 73)" includes examples of how individual software elements can be versioned. Change control of various elements is explained in chapter "Audit trail and change control (Page 113)" and chapter "Configuration control (Page 147)".

Always consult the plant operator to agree upon a procedure for making changes to a plant in ongoing operation; see chapter "Operational change control (Page 164)".

See also

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

Protecting the configuration

Besides controlling the configuration as part of the change process, the system including configuration must be protected from unintentional or unauthorized interventions. This is done by a combination of different measures. This includes, among others:

- Physical as well as logical access restrictions
- Password protection of the CPU
- Write protection for projects and charts
- Suitable procedures and training of employees

5.8 Versioning of software elements

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

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

However, whether the main version or the sub version is to be changed can also depend on the scope or effect of the change in question.

Note

The version, author, and comment fields can be written using the Import/Export Assistant (IEA) .

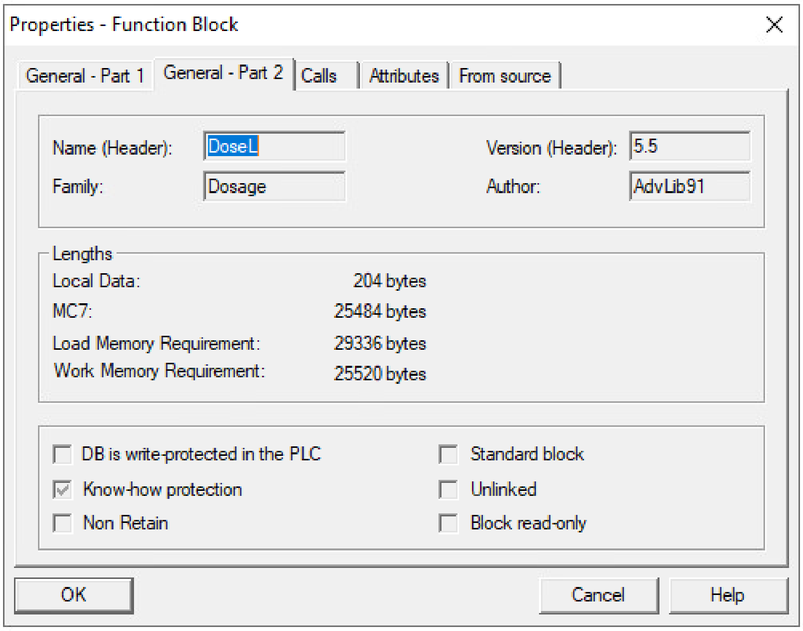
The following chapters show various examples of software element versioning, which are basically divided into:

- AS elements, which act as control functions in the controller
- OS elements, which are used for operator control and monitoring

5.8.1 Versioning of AS elements in PCS 7

The individual configuration levels in PCS 7 provide various options for assigning a version ID and, possibly, an author and comment to each element.

For blocks, CFCs, and SFCs, as well as for SFC types and models, the version numbers are managed in the properties of the respective object.



Properties - Function Block

Name (Header): DoseL

Version (Header): 5.5

Family: Dosage

Author: AdvLib91

Lengths

Local Data:	204 bytes
MC7:	25484 bytes
Load Memory Requirement:	29336 bytes
Work Memory Requirement:	25520 bytes

□ DB is write-protected in the PLC

☑ Know-how protection

□ Non Retain

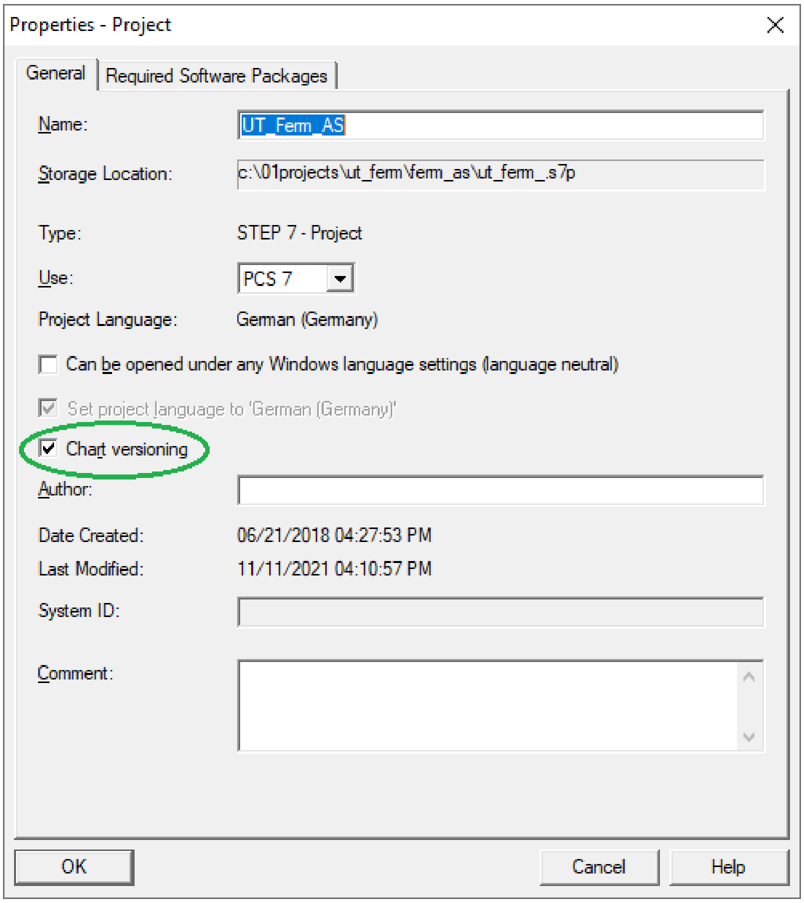
□ Standard block

□ Unlinked

□ Block read-only

Versioning of blocks, CFCs and SFCs

PCS 7 supports the option for semi-automatic versioning of CFC/SFCs and SFC types. This versioning must be enabled in the properties of the particular project or multiproject.



Name: UT_Ferm_AS

Storage Location: c:\01projects\ut_ferm\ferm_as\ut_ferm_.s7p

Type: STEP 7 - Project

Use: PCS 7

Project Language: German (Germany)

☐ Can be opened under any Windows language settings (language neutral)

☑ Set project language to 'German (Germany)'

☑ Chart versioning

Author:

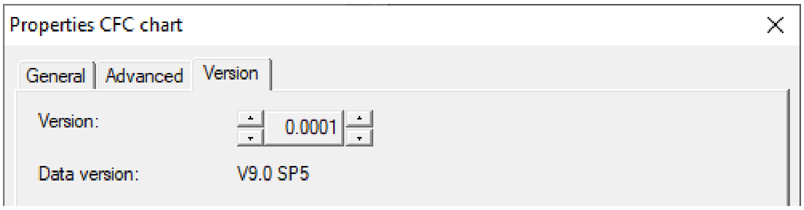
Date Created: 06/21/2018 04:27:53 PM

Last Modified: 11/11/2021 04:10:57 PM

System ID:

Comment:

When the versioning for the respective project is enabled, a dialog box opens automatically when you close a modified CFC/SFC or SFC type. In the example below this is the "Properties CFC Chart" dialog.



Version: 0.0001

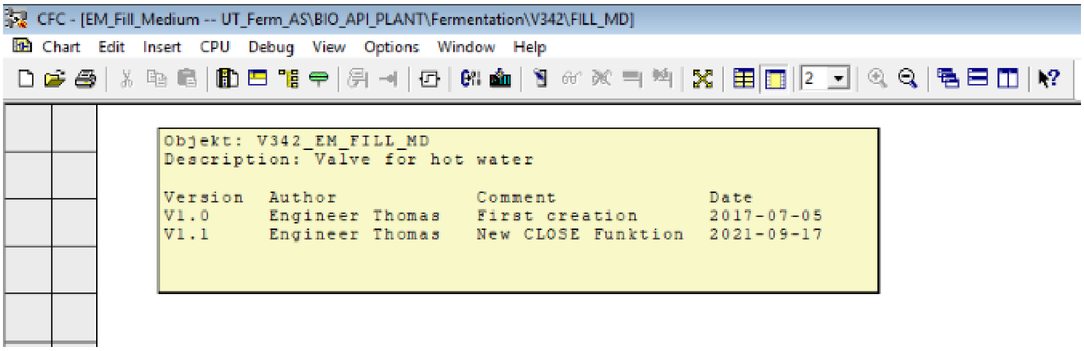
Data version: V9.0 SP5

Use the right and left cursor keys of the version number to increment the minor or major version. If you make an incorrect entry, the version can only be decremented to the last saved version. Changes to the version number must always be performed on the engineer's responsibility.

Note

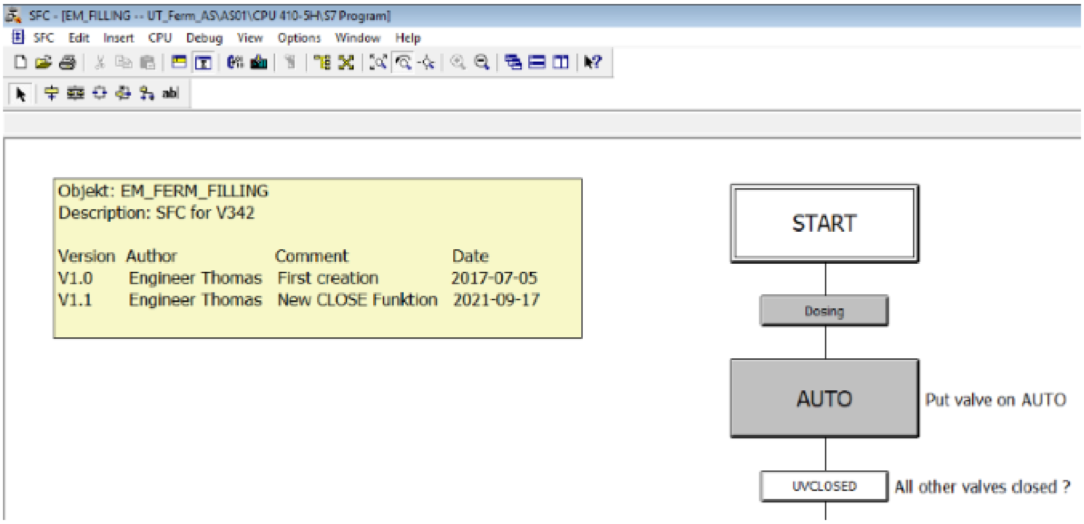
Once saved, a version number can no longer be reversed. The project team member must carefully examine their entries before confirming with OK. The version number can be set in the range of 0.0001 to 255.4095.

Information on the version history can also be added to the chart as a separate comment in the form of a text field, see graphic below.


CFC - [EM_Fill_Medium -- UT_Ferm_AS\BIO_API_PLANT\Fermentation\V342\FILL_MD]
Chart Edit Insert CPU Debug View Options Window Help
2

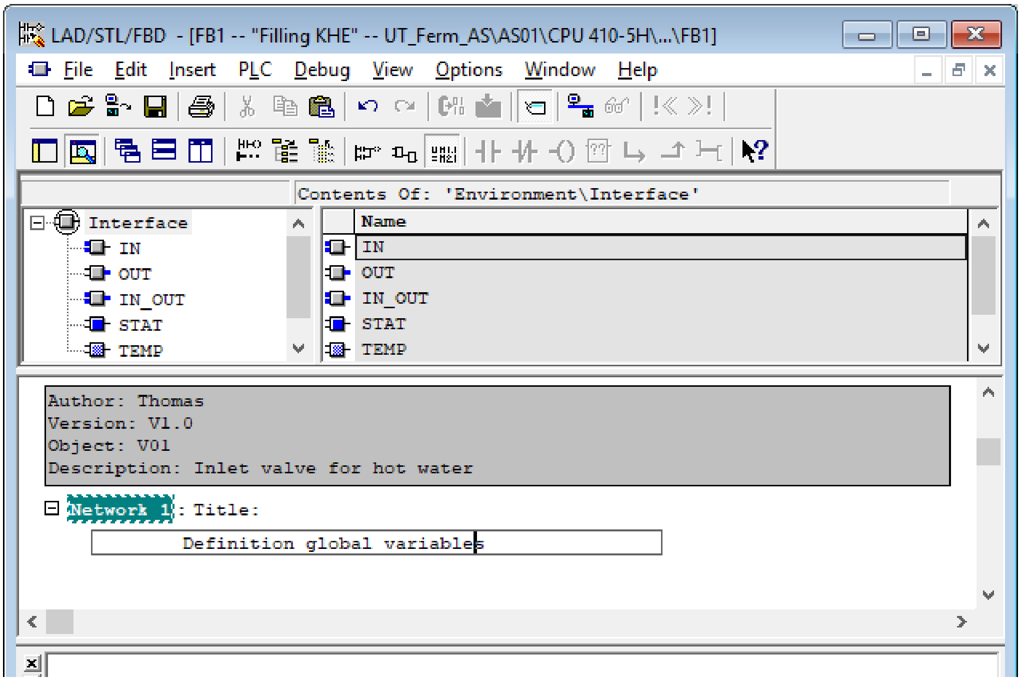
```
Objekt: V342_EM_FILL_MD
Description: Valve for hot water

Version  Author           Comment            Date
V1.0     Engineer Thomas  First creation     2017-07-05
V1.1     Engineer Thomas  New CLOSE Funktion 2021-09-17
```


SFC - [EM_FILLING -- UT_Ferm_AS\AS01\CPU 410-5H\S7 Program]
SFC Edit Insert CPU Debug View Options Window Help
START
Dosing
AUTO
Put valve on AUTO
UVCLOSED
All other valves closed ?

```
Objekt: EM_FERM_FILLING
Description: SFC for V342

Version  Author           Comment             Date
V1.0     Engineer Thomas  First creation      2017-07-05
V1.1     Engineer Thomas  New CLOSE Funktion  2021-09-17
```


LAD/STL/FBD - [FB1 -- "Filling KHE" -- UT_Ferm_AS\AS01\CPU 410-5H\...\FB1]
File Edit Insert PLC Debug View Options Window Help

Contents Of: 'Environment\Interface'

- Interface
  - IN
  - OUT
  - IN_OUT
  - STAT
  - TEMP

Name
IN
OUT
IN_OUT
STAT
TEMP

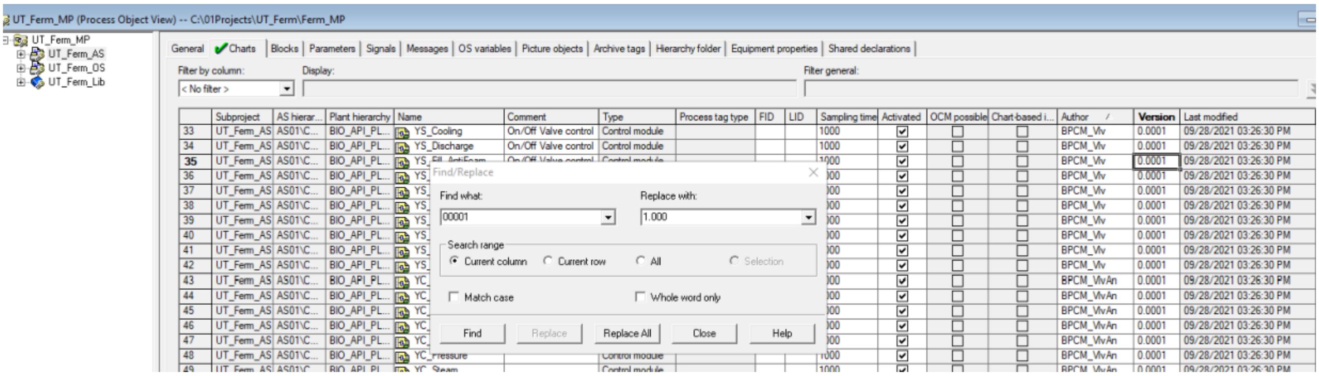
```
Author: Thomas
Version: V1.0
Object: V01
Description: Inlet valve for hot water
```

Network 1: Title:

Definition global variables

Note

Another possible variant is versioning on the unit level, if the plant has an appropriate structure. The unit and lower-level elements are managed and versioned as functional units. The version of the unit can be transferred to all elements using the "Find/Replace" function in the process object view. See the following screenshot. Version and change comments must then be maintained in the unit CFC.



Filter by column: < No filter >

Display:

Filter general:

	Subproject	AS hierar...	Plant hierarchy	Name	Comment	Type	Process tag type	FID	LID	Sampling time	Activated	OCM possible	Chart-based i...	Author	Version	Last modified
33	UT_Ferm_AS	AS01\C...	BIO_API_PL...	YS_Cooling	On/Off Valve control	Control module				1000	☑	☐	☐	BPCM_Vlv	0.0001	09/28/2021 03:26:30 PM
34	UT_Ferm_AS	AS01\C...	BIO_API_PL...	YS_Discharge	On/Off Valve control	Control module				1000	☑	☐	☐	BPCM_Vlv	0.0001	09/28/2021 03:26:30 PM
35	UT_Ferm_AS	AS01\C...	BIO_API_PL...	YS_Fill_AntiFoam	On/Off Valve control	Control module				1000	☑	☐	☐	BPCM_Vlv	0.0001	09/28/2021 03:26:30 PM
36	UT_Ferm_AS	AS01\C...	BIO_API_PL...	YS_						00	☑	☐	☐	BPCM_Vlv	0.0001	09/28/2021 03:26:30 PM
37	UT_Ferm_AS	AS01\C...	BIO_API_PL...	YS_						00	☑	☐	☐	BPCM_Vlv	0.0001	09/28/2021 03:26:30 PM
38	UT_Ferm_AS	AS01\C...	BIO_API_PL...	YS_						00	☑	☐	☐	BPCM_Vlv	0.0001	09/28/2021 03:26:30 PM
39	UT_Ferm_AS	AS01\C...	BIO_API_PL...	YS_						00	☑	☐	☐	BPCM_Vlv	0.0001	09/28/2021 03:26:30 PM
40	UT_Ferm_AS	AS01\C...	BIO_API_PL...	YS_						00	☑	☐	☐	BPCM_Vlv	0.0001	09/28/2021 03:26:30 PM
41	UT_Ferm_AS	AS01\C...	BIO_API_PL...	YS_						00	☑	☐	☐	BPCM_Vlv	0.0001	09/28/2021 03:26:30 PM
42	UT_Ferm_AS	AS01\C...	BIO_API_PL...	YS_						00	☑	☐	☐	BPCM_Vlv	0.0001	09/28/2021 03:26:30 PM
43	UT_Ferm_AS	AS01\C...	BIO_API_PL...	YC_						00	☑	☐	☐	BPCM_VlvAn	0.0001	09/28/2021 03:26:30 PM
44	UT_Ferm_AS	AS01\C...	BIO_API_PL...	YC_						00	☑	☐	☐	BPCM_VlvAn	0.0001	09/28/2021 03:26:30 PM
45	UT_Ferm_AS	AS01\C...	BIO_API_PL...	YC_						00	☑	☐	☐	BPCM_VlvAn	0.0001	09/28/2021 03:26:30 PM
46	UT_Ferm_AS	AS01\C...	BIO_API_PL...	YC_						00	☑	☐	☐	BPCM_VlvAn	0.0001	09/28/2021 03:26:30 PM
47	UT_Ferm_AS	AS01\C...	BIO_API_PL...	YC_						00	☑	☐	☐	BPCM_VlvAn	0.0001	09/28/2021 03:26:30 PM
48	UT_Ferm_AS	AS01\C...	BIO_API_PL...	YC_Pressure		Control module				1000	☑	☐	☐	BPCM_VlvAn	0.0001	09/28/2021 03:26:30 PM
49	UT_Ferm_AS	AS01\C...	BIO_API_PL...	YC_Steam		Control module				1000	☑	☐	☐	BPCM_VlvAn	0.0001	09/28/2021 03:26:30 PM

Find/Replace

Find what: 00001

Replace with: 1.000

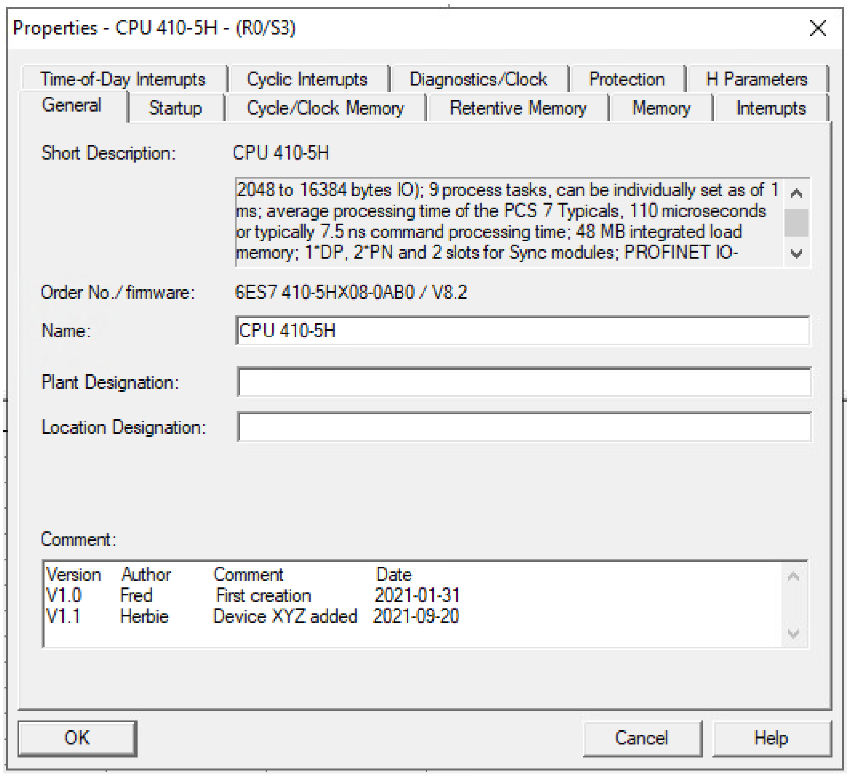
Search range: ● Current column ○ Current row ○ All ○ Selection

☐ Match case ☐ Whole word only

In addition, the configuration can also be controlled and versioned on a higher project or sub-project level. The corresponding tools as described in chapter "Configuration control (Page 147)" will be helpful in this regard.

Changes are always subject to a change request with the required change documentation attached.

Versioning of hardware configuration in "HW Config"



Short Description: CPU 410-5H

2048 to 16384 bytes IO); 9 process tasks, can be individually set as of 1 ms; average processing time of the PCS 7 Typicals, 110 microseconds or typically 7.5 ns command processing time; 48 MB integrated load memory; 1*DP, 2*PN and 2 slots for Sync modules; PROFINET IO-

Order No./firmware: 6ES7 410-5HX08-0AB0 / V8.2

Name: CPU 410-5H

Plant Designation:

Location Designation:

Comment:

Version	Author	Comment	Date
V1.0	Fred	First creation	2021-01-31
V1.1	Herbie	Device XYZ added	2021-09-20

In the "Properties" mask, the comment field can be used to enter the version ID and additional information, such as the version history.

Versioning of configuration in SIMATIC NET

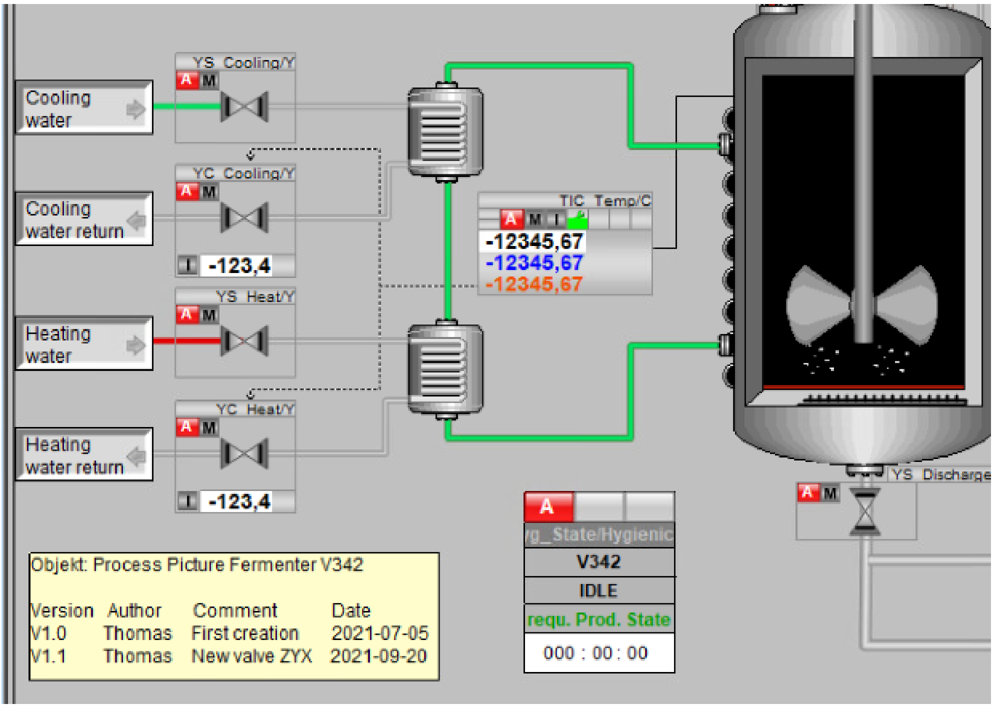
The version ID can be entered in the properties on the bus level (system bus, PROFIBUS).

5.8.2 Versioning of OS elements in PCS 7

During software creation, all graphics, reports, C scripts, and VB scripts created by the user must be assigned data such as an author, date, comment, and version ID. User objects (picture typicals), for example, feature a version field for this purpose. Scripts and user FBs (SCL) can be identified by means of their date of change; the version ID and comment must be inserted in the script header in text format.

Configuration settings must be appropriately documented, on the one hand to act as a reference for use in validation, and on the other hand to ensure they are available if the system needs to be restored.

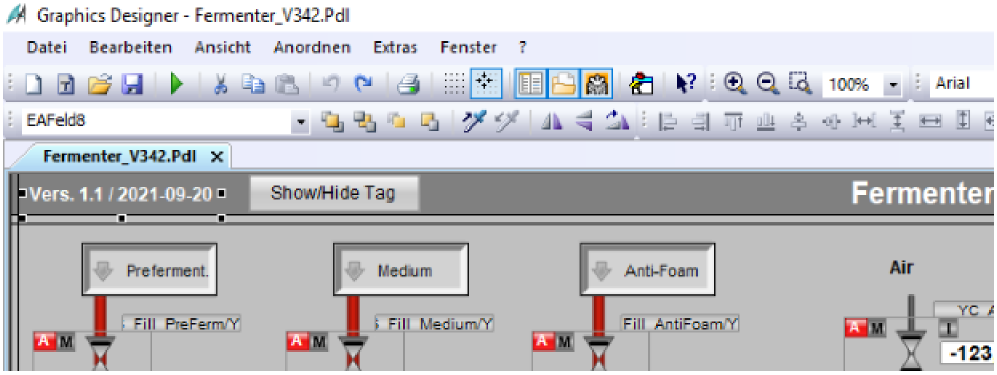
Examples for versioning graphic images



Objekt: Process Picture Fermenter V342

Version	Author	Comment	Date
V1.0	Thomas	First creation	2021-07-05
V1.1	Thomas	New valve ZYX	2021-09-20

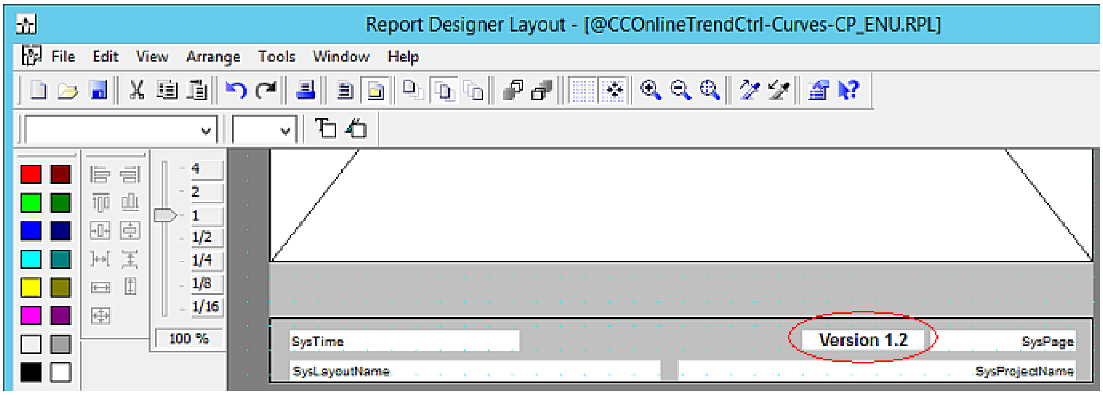
Versioning in a hidden field within the graphic display



Vers. 1.1 / 2021-09-20

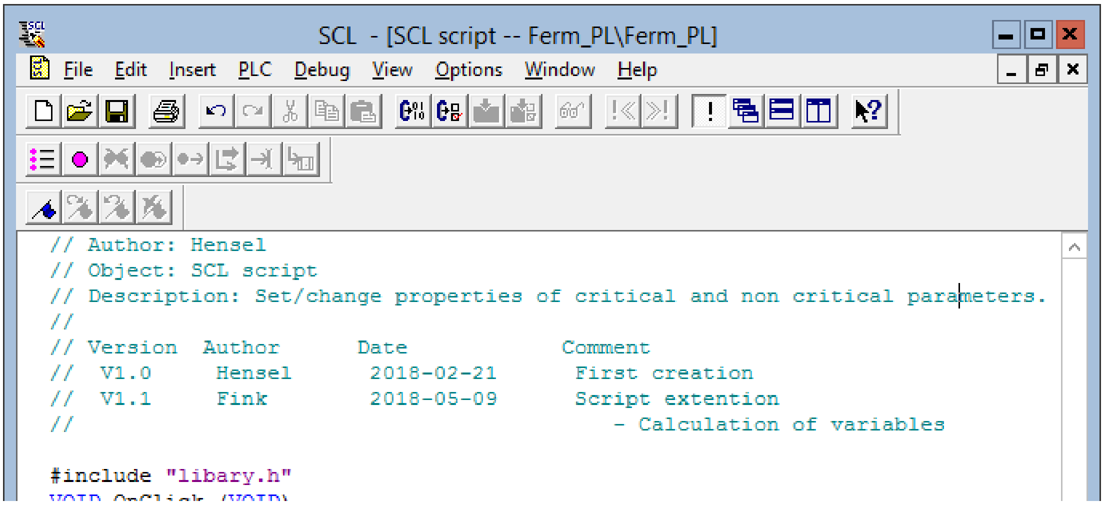
Version ID as a visible field within the graphic display; explanations relating to the version history outside it

Example for reports


Report Designer Layout - [@CCOnlineTrendCtrl-Curves-CP_ENU.RPL]
File Edit View Arrange Tools Window Help
4
2
1
1/2
1/4
1/8
1/16
100 %
SysTime
Version 1.2
SysPage
SysLayoutName
SysProjectName

Visible text field for versioning, e.g. in the report footer

Example for C/VB scripts


SCL - [SCL script -- Ferm_PL\Ferm_PL]
File Edit Insert PLC Debug View Options Window Help

```
// Author: Hensel
// Object: SCL script
// Description: Set/change properties of critical and non critical parameters.
//
// Version  Author      Date            Comment
//  V1.0     Hensel      2018-02-21      First creation
//  V1.1     Fink        2018-05-09      Script extention
//                                          - Calculation of variables

#include "libary.h"
VOID OnClick (VOID)
```

Inserting of version and comments within a script

5.8.3 Additional information on versioning

Versioning of BATCH elements

Recipe versioning is described under "Change Control for Recipes" in chapter "SIMATIC BATCH (Page 117)".

Versioning of projects, multiprojects, and libraries

Supporting system functions for versioning of projects, etc. are described in chapter "Configuration control (Page 147)".

Creating Application Software 6

This chapter presents information and recommendations intended to aid in the creation of application software in environments subject to GMP.

6.1 Software modules, types and copy templates

Software modules or type templates in the form of function blocks, function charts or complex step sequences are widespread in the process control engineering. You can create them in advance and reproduce them within the scope of the configuration.

Note

Modules and types are defined with the aim of not only reducing the amount of configuration work required but also, and more importantly, of creating a clear software structure. This helps to simplify the associated documentation and a risk-based definition of the testing work involved, while also supporting subsequent system maintenance.

See also

- Using types for programming in chapter "Software creation (Page 18)".

6.1.1 Modules and types in PCS 7

SIMATIC PCS 7 offers the possibility to create and centrally maintain templates for various types of software elements, see chapter "Using the master data library" (Page 59). The most important technological differences are the following:

Process tag type / **Control module (type)**	**Project-specific interconnection of blocks** Use of CFC technology, e.g. for functions such as • Valves • Pumps • Motors
Equipment module (type)	**Graphic configuration of sequential control systems** Type instance concept using the master data library Use of SFC technology, e.g. for recipe functions such as • Heating • Stirring (agitation) • Emptying

Equipment phase (type)	**Controls several lower-level equipment modules** Type-instance concept via the master data library, use e.g. • Vessels
Model solution	**Combination of several CFCs and/or SFCs** Use e.g. for functions such as • PID tempering of a tank • Level monitoring, including safety shutdown to protect against overflow of tank • Unit

The way the modules work must be described in a specification. The project-specific parameter assignments (archiving, block comment, measuring range, alarms and messages, MES-relevant, etc.) and interconnections must be defined.

Note

Modules are named in accordance with the Functional Specification and the Design Specification.

The modules/types must be verified and approved by means of a module test before they are duplicated.

An up-to-date record of the software modules used must be kept for each AS, in the form of a document containing software version details.

Process tag type

With SIMATIC PCS 7, a process tag type as a template consisting of one or more CFCs can be created for subcomponents of the same type. Creating process tag types for similar plant units saves on work required for engineering and testing. After testing, a process tag type can be duplicated as often as desired in the multiproject. For each replica, the plant hierarchy, CFC name, messages, I/Os for parameters or signals, and various module properties can be adapted.

Types for control module (CM)

A control module type (CMT) represents a closed process unit (e.g. valve) and serves as a type definition for control modules (CMs). Optional blocks (e.g. input/output block drivers) can be used to create variants of the CMT. This reduces the total number of types that must be made available and maintained. The CM instance can be individually adapted to the specific requirements after instantiating the variant. Changes to the type or variant can be passed on to the instance(s).

A CMT also has an automation interface that is used for data exchange between the PCS 7 project and the PAA (Plant Automation Accelerator) project as well as SIMATIC SIMIT.

See also

- Manual "PCS 7 Engineering System", chapter 9.15.6 and chapter 14 "Technological configuration", Online Support under entry ID 109800500 (https://support.industry.siemens.com/cs/ww/en/view/109800500)

Note

Existing process tag types can be converted to CMTs and configured via PAA within the framework of Integrated Engineering. Data exchange of pure CFC charts between SIMATIC PCS 7 and PAA is not possible; only information from the automation interface is exchanged here. Changing to engineering with CM(T)s is therefore recommended.

SFC type

The SIMATIC PCS 7 type/instance concept enables types of sequential controls to be created. The "SFC type" allows sequential controls to be defined, including an interface in the form of a CFC block. The sequence logic of the SFC type is based on the interface I/Os of the SFC type, i.e. in contrast to an SFC, an SFC type cannot access just any process signals.

The SFC type is not executable on its own. Like a function block type, an SFC type must be placed in a CFC to obtain a sequence-relevant object, in this case, an SFC instance. The SFC type and the SFC instances are included in the "Compile program" operation. To execute an SFC instance, both the SFC type and the SFC instance are downloaded to the automation system.

See also

- Manual "SFC for SIMATIC S7", Online Support under entry ID 109792631 (https://support.industry.siemens.com/cs/ww/en/view/109792631)
- Manual "PCS 7 Engineering Compendium Part C", chapter 6, Online Support under entry ID 109804258 (https://support.industry.siemens.com/cs/ww/en/view/109804258)

Types for equipment modules (EM) and equipment phases (EPH)

Similar to CMTs, equipment modules and equipment phases use the type-instance concept and are instantiated in the project via the respective EMT or EPHT types. A "sequential control system" is precisely one component of a equipment module, see SFC type. A control module (CM or CMT) is used to assign the equipment module to the sensors and actuators on the control-loop level.

Equipment phases control several lower-level equipment modules.

See also

- Manual "PCS 7 Engineering Compendium Part C", chapter 10, Online Support under entry ID 109804258 (https://support.industry.siemens.com/cs/ww/en/view/109804258)
- Manual "CFC for SIMATIC S7" chapter 10.13 "Configuring equipment modules", Online Support under entry ID 109792630 (https://support.industry.siemens.com/cs/ww/en/view/109792630)

Model solution

With SIMATIC PCS 7, a model consisting of one or more CFC and/or SFCs can be created for subcomponents of the same type. Creating models for similar plant units saves on work required for engineering and testing. After testing, a model can be duplicated as often as desired in a multiproject. For each replica, the plant hierarchy, CFC name, messages, I/Os for parameters or signals, and various module properties can be adapted. Models can also contain pictures and reports.

Each block instance can also be assigned a picture icon, which can then be automatically inserted, along with its tag interface, into the flow chart defined in the SIMATIC Manager by deriving it from the screen hierarchy during OS compilation. This saves work and ensures that the picture icon is connected to the correct block instance.

See chapter "Automatic generation of block icons (Page 84) " for information on using block icons.

Note

The block icons should be tested together with the associated software module as a process tag type and approved by the customer before they are duplicated.

6.1.2 Example of a process tag type

Every software module is created as a template in the form of a CFC. Following a software module test, this is released for instantiation and can be used within the framework of the configuration.

The "PCS 7 Compendium Part A" manual shows an example for such a module.

In accordance with GMP requirements, the parameter assignment and the interconnection of the inputs and outputs must be described in detail in a suitable specification ("Software Module Design Specification", for example) and verified by means of a test ("software module test" or "typical test").

See also

- Manual "PCS 7 Compendium Part A", chapter 8.2.1 "Process tag types (templates)", Online Support under entry ID 109809015 (https://support.industry.siemens.com/cs/ww/en/view/109809015).

Note

Consideration can also be given to the settings like process value archiving, for example, when creating the process tag type.

6.1.3 Automatic generation of block icons

Graphic block icons are used to display information relating to process states (e.g. valve open, closed, faulty, etc.) on the PCS 7 operator station (OS).

PCS 7 offers graphic templates for all blocks contained in the PCS 7 library, thus supporting the type/instance concept from the function block in the AS through to the operator component in the PCS 7 OS plant pictures. PCS 7 provides several templates for use.

Note

Generating block icons automatically reduces the risk of an error occurring.

See also

- PCS 7 on Tour – Basic,
  Chapter 10 section 5 "Adapted block icons and faceplates"
- Manual "PCS 7 Operator Station", chapter 10.2, Online Support under
  entry ID 109794374 (https://support.industry.siemens.com/cs/ww/en/view/109794374)

If the *Create/Update Block Icons* function is executed, the block icons are derived from the plant hierarchy of the project by means of their names and priorities, copied from the templates, and automatically linked to the tag interface of the relevant operator panel.

Priority	Picture name	Comment
1.	@PCS7Typicals_MyAPL.pdl	Starting with the picture which comes last alphabetically
2.	@PCS7TypicalsAPLV9.pdl	contained in the standard
3.	@PCS7TypicalsAPLV8.pdl	

The @PCS7TypicalsAPL<Version>.pdl template

The picture "@PCS7TypicalsAPL<Version>.pdl" is contained in every PCS 7 OS project as standard. It contains the standard block icons.

Note

The original "@PCS7TypicalsAPL<Version>.pdl" file must not be changed under any circumstances. Any changes to the original file will be overwritten when an update or upgrade is performed.

Separate templates should be created for customer-specific block icons, "@PCS7Typicals_MyAPL.pdl".

Project-specific template

A project-specific template, "@PCS7Typicals_MyAPL.pdl", can be created by copying the template "@PCS7TypicalsAPL<Version>.pdl". Customer-specific changes can then be made to the "new" template.

The @Template.pdl template

The "@TemplateAPL<Version>.pdl" template is primarily used when block icons are inserted into pictures manually. These block icons are not connected to the plant hierarchy and are not, therefore, created or updated by the system.

As a result, it can be helpful to use the template file. On the one hand you are not then linked to the plant hierarchy, and on the other hand you can use a wizard to export picture objects from one or all flow charts to a configuration file, modify block icons and their connections, and finally import the picture objects again. The configuration file can be edited using tools such as Excel.

Note

The "@TemplateAPL<Version>.pdl" file is maintained by the PCS 7 system and is overwritten when an update or upgrade is performed. It is therefore advisable to back up the "@TemplateAPL<Version>.pdl" file on a regular basis.

Other Template Pictures

@@ConfigTypicals.pdl

Used to create/update lifebeat monitoring.

@@MaintenanceTypicals.pdl

Used to create/update diagnostic pictures.

@PCS7elementsAPL.pdl
The template contains a collection of predefined objects for creating block icons.

@PCS7Typicals_Batch.pdl

Used to create/update block icons for SIMATIC BATCH.

@PCS7Typicalsrc.pdl

Used to create/update block icons for SIMATIC Route Control.

This list is not exhaustive.

Central changeability of picture objects

In the type definition, SIMATIC PCS 7 allows objects to be changed centrally; in other words, subsequent changes to picture objects are made in the template pictures.

Note

The central changeability of picture objects does not mean that changes are automatically passed on/down to the instances. As a result, the "Export Picture Objects" function must be executed via the dynamic wizard before the changes are passed on; this ensures that all objects will be located at their original positions after "Import Picture Objects" is performed.

Transfer of user-specific adaptations

If a custom template whose block icons are based on the APL is used in the project, these can also be migrated following an upgrade. In the migration case, the modified properties are kept and new functions or components from the @PCS7TypicalsAPLV9.pdl template are applied.

See also

- Manual "PCS 7 Compendium Part A", chapter 10.2.4 "Custom block icons/user objects", Online Support under entry ID 109809015 (https://support.industry.siemens.com/cs/ww/en/view/109809015).

6.1.4 Type Change in RUN (TCiR)

TCiR enables changes to block connections (inputs, outputs) to be downloaded from blocks in running operation. Due to the necessary validation procedures in the pharmaceutical industry, this functionality is only beneficial to a limited extent because, as with any change, its effects must be evaluated and verified. A possible application could, for example, be an ultra-pure water plant in a group of plants.

6.2 Bulk engineering

6.2.1 Bulk engineering with the process object view

If many parameters are to be checked or changed quickly, this can be done in the process object view. Using this, parameters can be filtered by certain criteria and their values viewed and processed.

The process object view enables the searching of charts throughout the entire multiproject.

6.2.2 Bulk engineering with the CM Generator

The CM Generator uses the bulk engineering mechanism to create, update and delete instances of CMTs, EMTs and EPHTs in a project using a list (referred to as "Generator list").

The CM Generator functionality is, for example, used for the following purposes:

- Generating control modules for process plants on the sensor and actuator level
- Generating equipment modules or equipment phases on the group control level (depending on the specified EMT/EPHT)

You can find a detailed description on the use of the CM Generator in the "PCS 7 Engineering System" manual.

See also

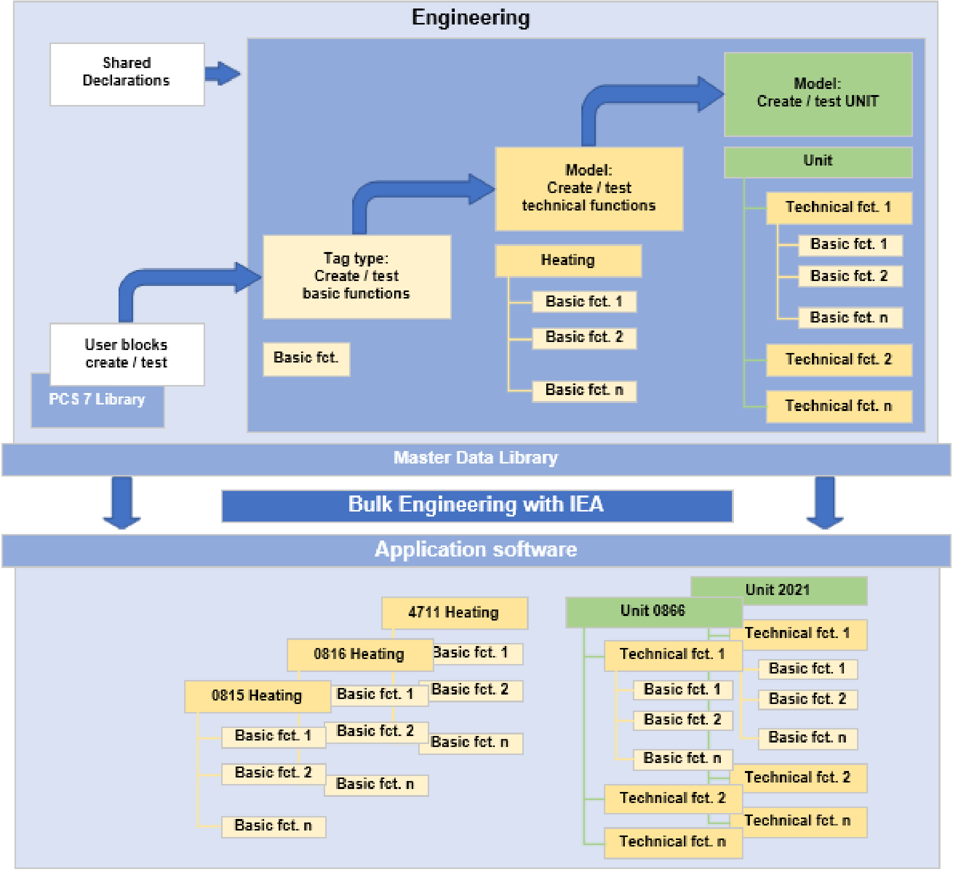
- Manual "PCS 7 Engineering System", chapter 14.9, Online Support under entry ID 109800500 (https://support.industry.siemens.com/cs/ww/en/view/109800500)

6.2.3 Bulk engineering with the IEA

The Import/Export Assistant (IEA) is used for two tasks.

Duplication with the IEA

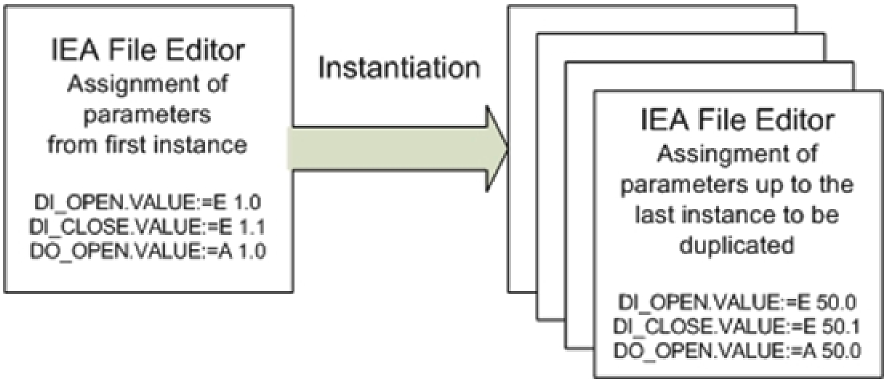
The Import/Export Assistant is used to duplicate process tag types or models. For this, project-dependent typicals are defined on the basis of standard libraries; these typicals can then be copied as instances as often as required using the Import/Export Assistant.



The modular software structure and the process of duplication using the IEA significantly reduce the engineering and testing effort required and thus the risk of errors occurring.

Parameter editing with the IEA

Furthermore, the IEA File Editor is used to enter parameters and signal processing in a table for each instance in accordance with the definitions contained in the specifications.



See also

- Manual "PCS 7 Engineering System", chapter 9.15.7 "Creating process tags from process tag types (multiproject)", Online Support under entry ID 109800500 (https://support.industry.siemens.com/cs/ww/en/view/109800500)
- Manual "PCS 7 Engineering System", chapter 10.3 and 10.4 "Working with the Import/Export Assistant", Online Support under entry ID 109800500 (https://support.industry.siemens.com/cs/ww/en/view/109800500)

6.2.4 Type/instance concept with the PAA

SIMATIC PCS 7 Plant Automation Accelerator (or PAA) is available for integrated engineering workflow of the process description up to the automation program. Like the IEA, the PAA is also an application for copying, editing, and importing software/hardware components using bulk engineering. In addition, the PAA also offers possibilities for documentation directly from the engineering tool as well as for document management including revisioning.

Existing project data can be transferred from SIMATIC PCS 7 to the PAA. An Excel import can be used to transfer process tag lists and signal lists to the PAA. The plant hierarchy, signal settings, and parameter settings can be adopted automatically from the imported process tag lists and signal lists. The hardware (distributed I/O including channel assignment) can be generated from signal lists. All software/hardware components configured in the PAA can then be transferred to SIMATIC PCS 7 and used there.

While duplication in the IEA is limited to copying (usually a one-time operation), the type/instance concept of the PAA also provides a tool for subsequent maintenance of types (control module types, CMT) and their associated instances (control modules, CM).

Comparison of the PAA with the IEA

User interface

PAA is based on COMOS and therefore has the same interface as the COMOS application. However, it is supplemented with various tools (PCS 7 Import/Export; Type Configurator, Excel

Import etc.). The working layer concept allows project editing to be assigned to different users who work in parallel on the project. This means that configuration with the PAA is also suitable for expanded configuration of existing plant components, but can also be used for pure hardware or software engineering.

Type/instance versus copying

If a typical is changed subsequently in the IEA, this requires a complete re-import of the "instances" (copies). This means that parameter assignments and interconnections to other functions or higher functions will be lost and that post-processing including validation is required.

The PAA enables you to make changes to the control module types (CMT) and update their instances (CM). Previously generated CMs can be checked for deviations from the CMT and the changes can be adopted. Incorrectly instantiated CMTs can be corrected with the 'Types Reassignment' tool. As result, configuring with CMTs is more flexible than configuring with IEA typicals.

Type variants with optional blocks

When configuring a CMT, it is possible to define optional blocks. Variants of the CMT can be created in the type configurator by selecting and deselecting these optional blocks. These variants are instantiated and can be post-processed like CMTs and their instances can be updated.

Thus, for example, a valve with an interlock block and another valve without an interlock block are generated from the same CMT. With the IEA, two typicals would be necessary for these two valves.

When the IEA is used, up to 8 typicals, depending on the combination, would have to created and tested, as opposed to a single CMT with, for example, three optional blocks.

Configuration with PAA

At the beginning, a project is created in PAA. For data exchange, a multiproject must first be created in SIMATIC PCS 7 and the master library must be defined. This can be imported into PAA, if it contains CMTs.

The PAA has its own user administration. This makes it possible to release pre-defined areas (working layers, projects, functions) for the user or to define different authorization levels.

Control Module Types (CMT)

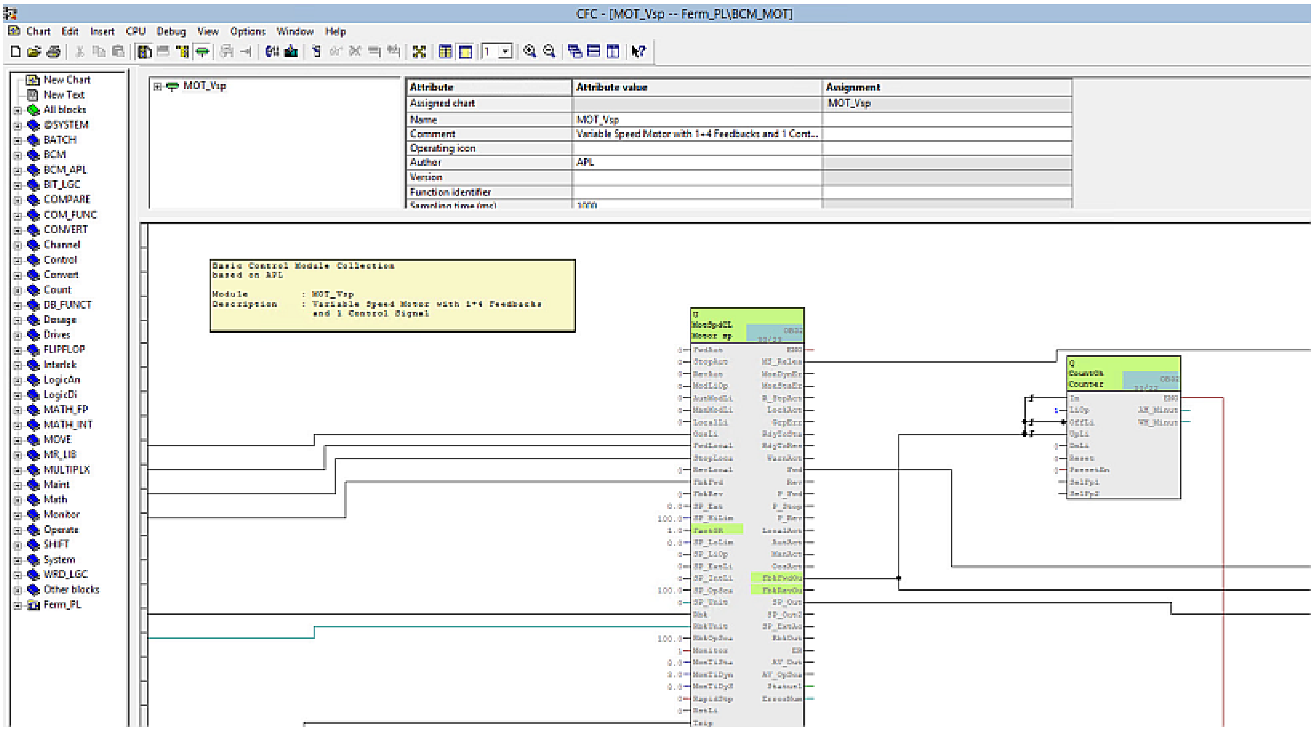
The user can generate CMTs from a process tag type from the master data library or create completely new CMTs. CMTs can contain individual control units, control tags, and messages. Both the green colored block headers in the following figure and the top area of the image illustrate that a CMT is involved.

Equipment Module Type (EMT)

This is done in the same way for equipment modules (EM) and equipment phases (EPH). Instead of interconnecting individual block I/Os, a CM instance fulfills a role from the point of view of the EM and the individual interconnections, which are of course still necessary, are performed automatically in the background. Neither equipment phase types (EPHTs) nor equipment module types (EMTs) are to be understood as a substitute for SFC types. Instead, they use the proven SFC type instance concept internally. An EPHT or EMT is like a CMT that contains exactly one instance of an SFC type. Other blocks may also be contained.

Note

Only the green-colored technological I/Os can be processed in the PAA. Of course, all inputs/outputs can still be processed in PCS 7. The idea behind this is that a type has certain static elements that should be the same in every instance. These are therefore not required for processing in PAA. The green inputs/outputs, in turn, represent the instance-specific inputs/outputs and parameters that can be processed.



Attribute	Attribute value	Assignment
Assigned chart		MOT_Vsp
Name	MOT_Vsp	
Comment	Variable Speed Motor with 1-4 Feedbacks and 1 Cont...	
Operating icon		
Author	APL	
Version		
Function identifier		
Sampling time (ms)	1000	

```
Basic Control Module Collection
based on APL

Module           : MOT_Vsp
Description      : Variable Speed Motor with 1-4 Feedbacks
                   and 1 Control Signal
```

CMTs, their attributes, control tags and messages can be processed in PAA.

CMs are generated by assigning a variant of the CMT in the plant hierarchy. When creating the variant, you can select whether and which optional blocks of the CMT are to be used.

After the project is processed in PAA, all relevant data are exported back to the PCS 7 project. Further processing of the project takes place in SIMATIC Manager.

See also

- "SIMATIC PCS 7 Plant Automation Accelerator", Online Support under entry ID 109742154 (https://support.industry.siemens.com/cs/ww/en/view/109742154)

6.3 Creating process pictures

Process pictures must be created in accordance with the definitions contained in the specifications (e.g. URS, FS, and P&ID). Similar to all the other work steps in the GMP environment, **planning** is performed first, followed by **implementation** and, subsequently, **testing**.

Block icons should be assigned using the "automatic generation of block icons" function, which means one block icon is assigned to each instance-specific module (valve, pump, closed-loop controller, etc.) in the process picture using the IEA file. The picture and the block charts must be configured in the same plant hierarchy folder, or in plant hierarchy folders with the same name, in order for block icons to be generated.

There are SVG graphics (scalable vector graphics) in SIMATIC PCS 7. These do not have a loss of quality when scaling the plant pictures and can therefore be output in good quality on different screen formats.

After the graphics are created, they should be submitted to the customer in the form of screenshots for approval.

See also

- Chapter "Automatic generation of block icons (Page 84)"
  for information on using template pictures as a library
- Manual "PCS 7 OS Process Control", chapter 8.3, Online Support under entry ID 109794375 (https://support.industry.siemens.com/cs/ww/en/view/109794375)
- Manual "PCS 7 Compendium Part A", chapter 10.2 "Visualization interface", Online Support under entry ID 109809015 (https://support.industry.siemens.com/cs/ww/en/view/109809015)

Note

When using the WinCC OnlineTableControls, "Permit editing" must be disabled in the properties so that the mask cannot be used to change values.

6.4 User-specific blocks and scripts

User-specific blocks (FB, FC) and scripts (C, VB) are programs written and created by the user, which are assigned to GAMP software category 5. This type of software was developed to meet customer-specific demands not covered by existing functions and libraries.

In general with such customized blocks and scripts, a greater effort for validation must be calculated in the form of detailed functional and interface descriptions as well as documented tests; see also chapter "Software categorization according to GAMP 5 Guide (Page 138)".

Note

When user-specific blocks and scripts are created, the rules for creating software elements should be defined in instructions specific to the project/department (coding standards, PCS 7 style guide, etc.).

See also

- Manual "PCS 7 APL Styleguide", Online Support under entry ID 65601446 (https://support.industry.siemens.com/cs/ww/en/view/65601446)
- Manual "PCS 7 Compendium Part A", chapter 8.1.2 "Creating user-defined technological blocks", Online Support under entry ID 109809015 (https://support.industry.siemens.com/cs/ww/en/view/109809015)

6.5 Interfaces to SIMATIC PCS 7

6.5.1 PCS 7 Web Option for OS

This option enables PCS 7 system processes to be controlled and monitored via an internet/intranet connection. One PCS 7 OS Web server and at least one PCS 7 Web client is required.

Within a PCS 7 OS multiple station system the PCS 7 OS Web server is installed as an OS client with PCS 7 OS Web server functionality. It should not also be used as an operator station (OS client). This can be ensured by deactivating graphics runtime.

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

The Web server itself should be certified so that access to Web server functions is secure, authenticated, and encrypted (keyword: https access).

All pictures and required scripts are stored on the OS Web server so that they can be displayed and run on the Web client. All pictures and scripts must be published. The "Web View Publisher" is used for this.

See also

- Manual "PCS 7 Web Option for OS", Online Support under entry ID 109794376 (https://support.industry.siemens.com/cs/ww/en/view/109794376)
- Manual "PCS 7 Compendium Part A", chapter 10.2 "Visualization interface", Online Support under entry ID 109809015 (https://support.industry.siemens.com/cs/ww/en/view/109809015)

Note

If scripts are used, preference should be given to event-controlled script editing wherever possible, as it saves on resources. By contrast, cyclic scripts should only be used on a specific basis as needed.

SIMATIC Logon must be installed on the Web server, thus integrating the Web client into the SIMATIC Logon functions. As a result, access to the Web client is password-protected. User permissions are assigned in the OS User Administrator. They correspond to those of standard clients, the only additional requirement is that the intranet/internet access option must be enabled.

See also

- Chapter "Information security and data integrity (Page 53)"
- Manual "Security Concept PCS 7 and WinCC", Online Support under entry ID 109780811 (https://support.industry.siemens.com/cs/ww/en/view/109780811)

Load balancing functionality

When several Web Navigator servers are used, the "Load Balancing" functionality enables an even load balance among the servers. In addition, the Web Clients are automatically redistributed among the other Web servers if one of the Web servers fails. This works by selecting a Load Balancing server in advance from the participating Web Navigation servers. If a Web Client then logs on to a Load Balancing server, this server assigns the Web Client to the server with the lowest load.

To make use of the Load Balancing functionality, it must be configured on each participating Web server. The WinCC Basic system and the Web Navigator server must be installed for this. The Web servers must be set up identically (applies also to the user administration), and the standard website must be set for Web Navigator.

The configuration of the Load Balancing function must be opened in WinCC Explorer using the shortcut menu of the Web Navigator. The window that opens must list each individual Web server using its IP address. For the Load Balancing server, the "Allow Load Balancing" check box must be selected and a polling interval must be set.

Note

Web servers with a "Web Navigator Diagnostics Server" license must not be listed as a Load Balancing participant.

The "WinCCViewerRT.exe" application does not support the "Load Balancing" function.

Thin Client

A thin client solution allows the terminal server and the Web server to be operated on one computer. In this case, a terminal session is opened on the terminal server for each thin client. The thin clients can then access the terminal server and Web server using the Remote Desktop Protocol (RDP). Because this is a server-based functionality, a user does not have to be logged on to the terminal server.

A thin client solution is easy to maintain because changes only have to be made once on the terminal server and are then available to every thin client.

See also

- Manual "Industrial Thin Clients", Online Support under entry ID 109801145 (https://support.industry.siemens.com/cs/ww/en/view/109801145)

WebUX

WebUX enables access to process pictures suitable for WebUX via an HTML 5-capable browser. The functionality is severely limited in comparison with the web client.

In the interests of process security, only encrypted HTTPS connections with SSL certificates are supported.

User rights that permit access to the WebUX server must be configured in the WinCC User Administrator in conjunction with SIMATIC Logon. For critical operations, in particular, read-only access is recommended.

See also

- Manual "WinCC Basic Options", Online Support under entry ID 109792604 (https://support.industry.siemens.com/cs/ww/en/view/109792604)

Note

The setting up of a web server may possibly enable access to your plant infrastructure. Protect the computer on which the web server is installed. Make sure that the following rules are followed:

- The computer can only be accessed via secured connections.
- The test mechanisms provided by software manufacturers are enabled and are never circumvented.

6.5.2 OS client in a virtual environment

On high-performance computers (see VMWare system requirements (https://www.vmware.com/resources/compatibility/search.php)) it is possible to create multiple virtual environments. These then serve as the basis for an OS Client, irrespective of the actual hardware. OS clients are released for use in a virtual environment.

When operating an OS client in a virtual environment, operator control and monitoring takes place via a Thin Client that is connected to the VMware ESXi platform. Multiple virtualizations can run simultaneously on the ESXi platform, but only one Remote Desktop connection per virtualization is possible. Up to 4 monitors can be connected by selecting the Thin Client. If a connection of USB devices to the OS client is required, the connection is made via the assigned Thin Client or a centrally managed USB device server.

See also

- Release of PCS 7 components for virtual environment, Online Support under entry ID 109795917 (https://support.industry.siemens.com/cs/ww/en/view/109795917)
- Manual "PCS 7 Virtualization - Configuration", Online Support under entry ID 109801455 (https://support.industry.siemens.com/cs/ww/en/view/109801455)
- GAMP Good Practice Guide "IT Infrastructure" 2nd Edition, chapter 19

6.5.3 Open PCS 7

Open PCS 7 makes PCS 7 data available to higher-level systems, such as the plant control level. The standard interfaces below are available for exchanging data between Open PCS 7 stations:

- OPC UA (Unified Architecture)
- OPC "Classic"
  - OPC DA (Data Access)
  - OPC A&E (Alarm & Events)
  - OPC HDA (Historical Data Access)
  - OPC H A&E (Historical Alarm & Events)
- OLE/DB for applications with OLE capability, such as MS Office products;
  OLE/DB permits access to historical values, alarms, and messages via standardized database calls

The Open PCS 7 station can be used to access several redundant server pairs. If the active server fails, the station switches to the remaining server automatically, so that this server carries out the next read job.

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

Access to the station	OPC interface	Data type
OS server	UA	Process values and messages
OS server	DA	Process picture tags
OS server	A&E	Alarms and messages
OS server	HDA	Historical measured values (Tag Logging)
OS server	H A&E	Historical alarms and messages (Alarm Logging)
OS server	OLE-DB	Direct access to archive data

See also

- Manual "OpenPCS 7", chapter 7.1 "Access options", Online Support under entry ID 109794368 (https://support.industry.siemens.com/cs/ww/en/view/109794368)

Advantages of OPC UA compared to previous OPC specifications are:

- Integrated security concept (authentication and authorization, encryption and data integrity)
- Independent of DCOM, no DCOM settings are required
- Independent of operating system, independent of manufacturer
- Harmonization of the previous OPC standards to form one interface; one common OPC standard for tags, alarms, and historical data
- Communication via a single firewall port

Note

The OPC connection should not serve as an extended operating source, but essentially as data evaluation or information. When establishing an OPC connection, particular emphasis must therefore be placed on data security and the assignment of write permissions. Visibility and write permissions can be configured individually for each OS tag.

The PCS 7 OS Web Option should be selected for possible operation from outside the PCS 7 environment, see chapter "PCS 7 Web Option for OS (Page 93)".

6.5.4 SIMATIC BATCH API

SIMATIC BATCH API (Application Programming Interface) offers the following function calls as a programming interface:

- Access to BATCH objects and data
- Navigate through SIMATIC BATCH object hierarchies
- Notifications about events

A field of application is the data interface for transmission of events and methods (e.g. CreateBatch, ArchiveBatch, GetParameter, etc.) to an MES or ERP levels.

6.6 Recipe control with SIMATIC BATCH

SIMATIC BATCH is a software package for SIMATIC PCS 7, which plans, monitors and controls discontinuous processes, known as batch processes.

A major advantage of the batch production is the collection and archiving of production data. These production data are needed for both the regulatory requirements for traceability (audit trail) as well as for operational analysis of the production process.

6.6.1 Definition of batch terminology

Some commonly used batch terminology is described below.

Term	Description
Master recipe	Set of rules and information required to define how a product is manufactured.
Control recipe	Copy of the master recipe with extra information specific to a process cell and corresponding scaling of the desired production quantity
Batch	Equipment-dependent amount of a product manufactured in a defined, discontinuous production sequence.
Process	A sequence of chemical, physical, or biological activities for manufacturing materials or products.

6.6.2 Conformity with the ISA-88.01 standard

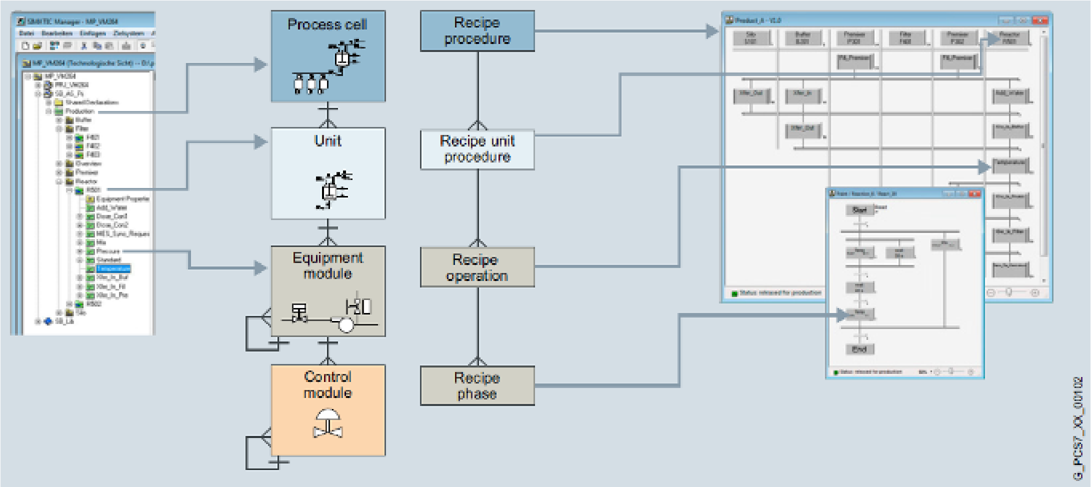
ISA-88 is an international standard for batch control, which represents the design specifications for software, equipment and operation of the processing. SIMATIC BATCH was developed on the basis of the *ANSI/ISA-88.00.01 (Batch Control, Part 1: Models and Terminology)* standard.

One of the recommendations contained in the "Technical Report" *ISA-TR88.0.03* is the use of SFC (Sequential Function Charts, DIN/IEC 1131) as a graphic language for describing recipe procedures. Recipes created with the SIMATIC BATCH Recipe Editor follow the structures and functionalities described in this standard.

SIMATIC BATCH makes production data available according to *ISA-88.00.04 (Batch Production Records)*.

SIMATIC PCS 7 software model

ISA-88.01 describes various models, which can be fully implemented with PCS 7 and SIMATIC BATCH.



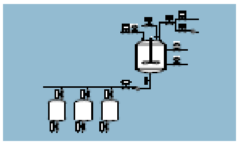
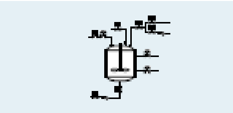
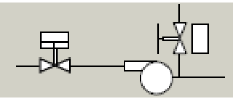
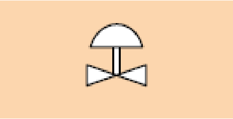
The **process cell model** (physical model) describes the process cell, unit, equipment module, and device control level, which is mapped using the plant hierarchy in the plant view of SIMATIC Manager.

In SIMATIC BATCH, the **procedural model** (procedure, unit procedure, operation, phase) reflects the process cell model from the point of view of the control sequence.

Term	Description
Recipe procedure	A recipe procedure runs in a process cell to control a process and to create a batch of a product.
Recipe unit procedure	A recipe unit procedure runs on a unit to control a recipe stage. A unit can only be occupied by one batch at any one time.
Recipe operation/ recipe phase	A recipe operation or a recipe phase runs on an equipment module to implement a process engineering task or function.
Control-loop level	The control-loop level is not within the scope of the BATCH system and is addressed only via the equipment module. It is entirely located in the automation system.

Application of the ISA-88.01 standard in SIMATIC PCS 7

The ISA-88.01 software model divides the process into various modules, simplifying the process of validation. The process is split up hierarchically into the following parts:

Physical model	Graphic	Procedural elements	Implementation in PCS 7	Implemented by
Process cell		Procedure	BATCH component: Recipe	Operator / supported by supplier
Unit		Unit procedure(s)	CFC component: Unit block BATCH component: Unit recipe	Operator / supported by supplier
Equipment module (EM)		Recipe operation / phase (may contain control strategies)	SFC type component: Use of SFC types to allow instantiation. (equipment phases, equipment operations)	Supplier / supported by the operator
Control module (CM)		-	CFC component: Use of the PCS 7 library and of CFCs.	Supplier

The SIMATIC PCS 7 Industry Library contains specific functions which enable an integrated and ISA-88 compliant engineering & operating concept including batch integration.

Note

The names and functions of the modules correspond to the definitions contained in the specifications.

See also

- Manual "PCS 7 SIMATIC BATCH", Online Support under entry ID 109794450 (https://support.industry.siemens.com/cs/ww/en/view/109794450)
- Application example "Engineering and automation of batch processes with PCS 7 along ISA-88 models", Online Support under entry ID 109784331 (https://support.industry.siemens.com/cs/ww/en/view/109784331)

6.6.3 Configuring SIMATIC BATCH

Basics and options of SIMATIC BATCH are explained in chapter "Software components for engineering (Page 30)".

See also

- Manual "Getting Started PCS 7 SIMATIC BATCH", Online Support under entry ID 109781909 (https://support.industry.siemens.com/cs/ww/en/view/109781909)
- Manual "PCS 7 Compendium Part C", Online Support under entry ID 109804258 (https://support.industry.siemens.com/cs/ww/en/view/109804258)

The individual configuring steps are divided into the following:

Working in SIMATIC Manager

The following steps, among others, are performed in the SIMATIC Manager:

- Creating and configuring batch systems (server, clients)
- Creating the plant hierarchy
- Compiling OS data
- Generating and propagating batch types
- Transferring data to OS
- Loading process cell data

Working in the BATCH Control Center (BCC) and Recipe Editor (RP)

Among other things, these steps are performed here:

- Reading / updating batch data
- Creating master recipes
- Creating the recipe structure
- Creating ROP libraries, formula categories and formulas
- Creating order category, order and batch(es)
- Releases for master recipes and completed batches
- Exporting/importing of recipes, parameter sets, etc.

See also

- Application examples for specification of equipment phases with SFC types as well as instantiation, Online Support under entry ID 33412955 (https://support.industry.siemens.com/cs/ww/en/view/33412955)

6.6.4 Functions and settings in SIMATIC BATCH

Various functions and project settings can be used in SIMATIC BATCH. A number of settings are presented in the following. The operating manual for SIMATIC BATCH provides detailed information.

Predefined batch names

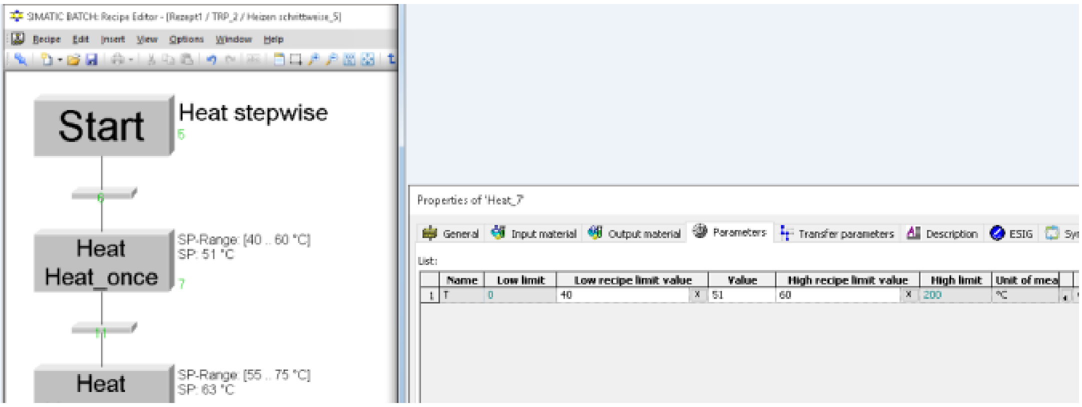
With the "Use predefined batch names" function, batch names can be automatically created from various static and dynamic elements.

Note

The length of the batch name is restricted to 32 characters.

Recipe step-specific setpoints

Within the defined equipment limits, the range for setpoints can also be limited for each recipe step. This means that the process can be guided better and the quality of the final product is increased.



List:

	Name	Low limit	Low recipe limit value	Value	High recipe limit value	High limit	Unit of mea
1	T	0	40	51	60	200	°C

Editing of recipes with "Release revoked/invalid" status

With the "No" setting, you prevent recipes in 'Release revoked/invalid' status from being re-released with the same name/version.

Note

The default setting is "Yes" and should be set to "No" in the regulated environment.

Automatically release batches

Newly added batches are automatically released upon creation for production. The default setting is "No". For the setting "Yes", the user saves a separate release step, which may make sense for other authorizations. A configured signature is requested for the release even when using automatic system release.

Exporting/importing of batch objects

For the export/import of

- Libraries
- Master recipes
- Formula categories and formulas

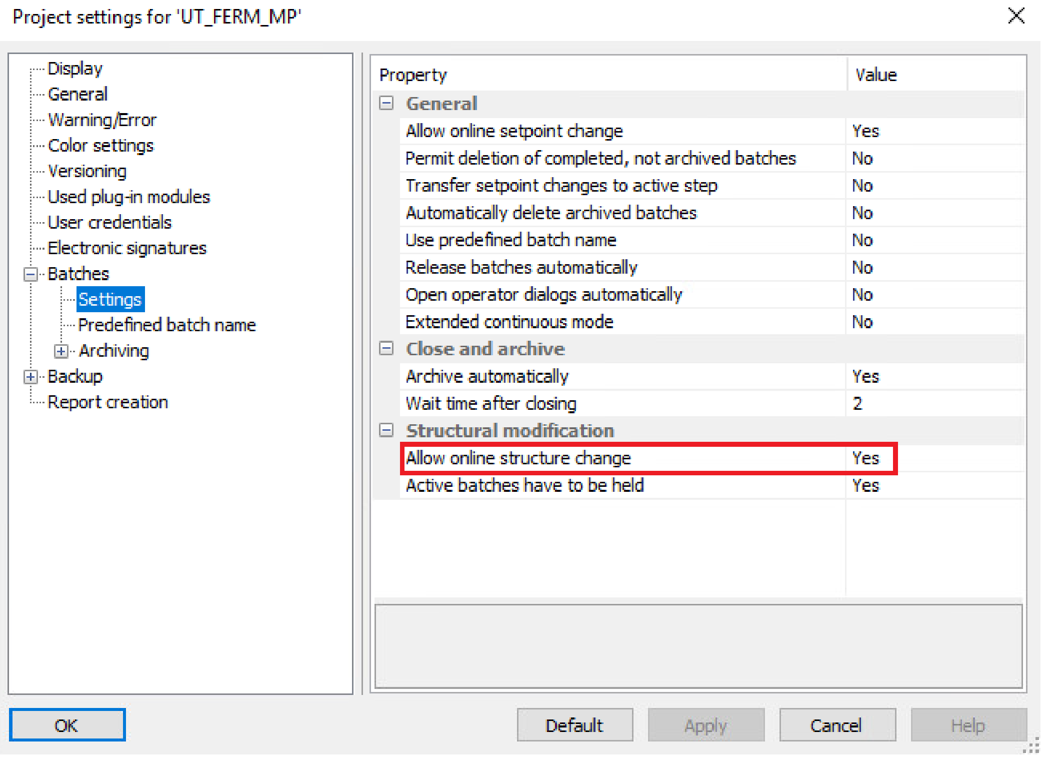
See manual "SIMATIC BATCH", chapter 9.5.8, Online Support under entry ID 109794450 (https://support.industry.siemens.com/cs/ww/en/view/109794450).

Online structure changes for recipe structures

SIMATIC BATCH allows you to change recipe structures online. This applies to control recipes that have the status "released", "planned" or "started".

The following conditions regarding settings apply:

- The master recipe has the status "Release for testing".
- The user must have the "structural changes" permission.
- "Allow online structure changes" must be set in the project settings.



Project settings for 'UT_FERM_MP'

Property	Value
General	
Allow online setpoint change	Yes
Permit deletion of completed, not archived batches	No
Transfer setpoint changes to active step	No
Automatically delete archived batches	No
Use predefined batch name	No
Release batches automatically	No
Open operator dialogs automatically	No
Extended continuous mode	No
Close and archive	
Archive automatically	Yes
Wait time after closing	2
Structural modification	
Allow online structure change	Yes
Active batches have to be held	Yes

Selecting the "Active batches have to be held" option provides protection by bringing the current batch to a safe state when changes are made to recipe structures. Once the change is made, the batch must be resumed by the operator.

Note

Online structural changes are an additional functionality for master recipes during testing. They serve to simplify the optimization of recipes. Online structural changes are not possible during production (master recipe released for production). The default setting is "No".

Notes and restrictions

- When online structure changes are being made to a batch, access to this batch by other clients is blocked. A visual comparison of the changes to all SIMATIC BATCH clients is made once the online structure changes are complete.
- It is advisable to stop the batch for structural changes.

If the "Active batches have to be held" option is disabled, the change can be made during ongoing operation, which has the disadvantage that the batch automatically applies and enables the changes when the changes are made.

Deleting a canceled batch

Attention should be given, for example, to the point "Permit deletion of completed, not archived batches". This means that canceled batches can be deleted without archiving the data. This is only rarely desired in the pharmaceutical environment. This setting should therefore remain deselected, unless the customer expressly requests otherwise.

Additional settings in SIMATIC BATCH

Important parameters and settings are also contained in

- Chapter "SIMATIC BATCH (Page 117)"
- Chapter "Electronic signature in SIMATIC BATCH (Page 122)"

6.6.5 Messages in SIMATIC BATCH

All messages for the batch control, which are managed in the WinCC archives, can also be displayed on the SIMATIC BATCH client. The requirement is that a PCS 7 OS application is running on the computer.

See also

- Manual "SIMATIC BATCH", chapter 9.8.7 "Operator and status messages" and chapter 15.1.2.3 "Warning and error messages", Online Support under entry ID 109794450 (https://support.industry.siemens.com/cs/ww/en/view/109794450)

6.6.6 Creating reports in SIMATIC BATCH

The SIMATIC BATCH report ensures the documentation of recipes and batch data in the form of logs:

- The recipe report contains all the data required for batch production. This includes the recipe header data, the input materials and output materials list and the procedural rules.
- The batch report contains all the information of the produced batch that is required for reproducibility of the batch process, quality assurance and fulfillment of legal requirements.
- The reports can be automatically saved as a PDF file.

The report is integrated in the user interface of the BATCH Control Center.

See also

- Manual "SIMATIC BATCH", chapter 9.5.7 and chapter 9.9, Online Support under entry ID 109794450 (https://support.industry.siemens.com/cs/ww/en/view/109794450)
- Creating Report Templates for the Information Server on the Process Historian Database, Online Support under entry ID 64906050 (https://support.industry.siemens.com/cs/ww/en/view/64906050)

6.7 SIMATIC Route Control

SIMATIC Route Control is a program package of SIMATIC PCS 7, which is used for management and automated control of the entire process route network of a production plant. Due to its matrix-based configuration, process routes can be flexibly determined and automatically controlled by means of different modes. One of the main applications of SIMATIC Route Control is the automated transport of materials in plants.

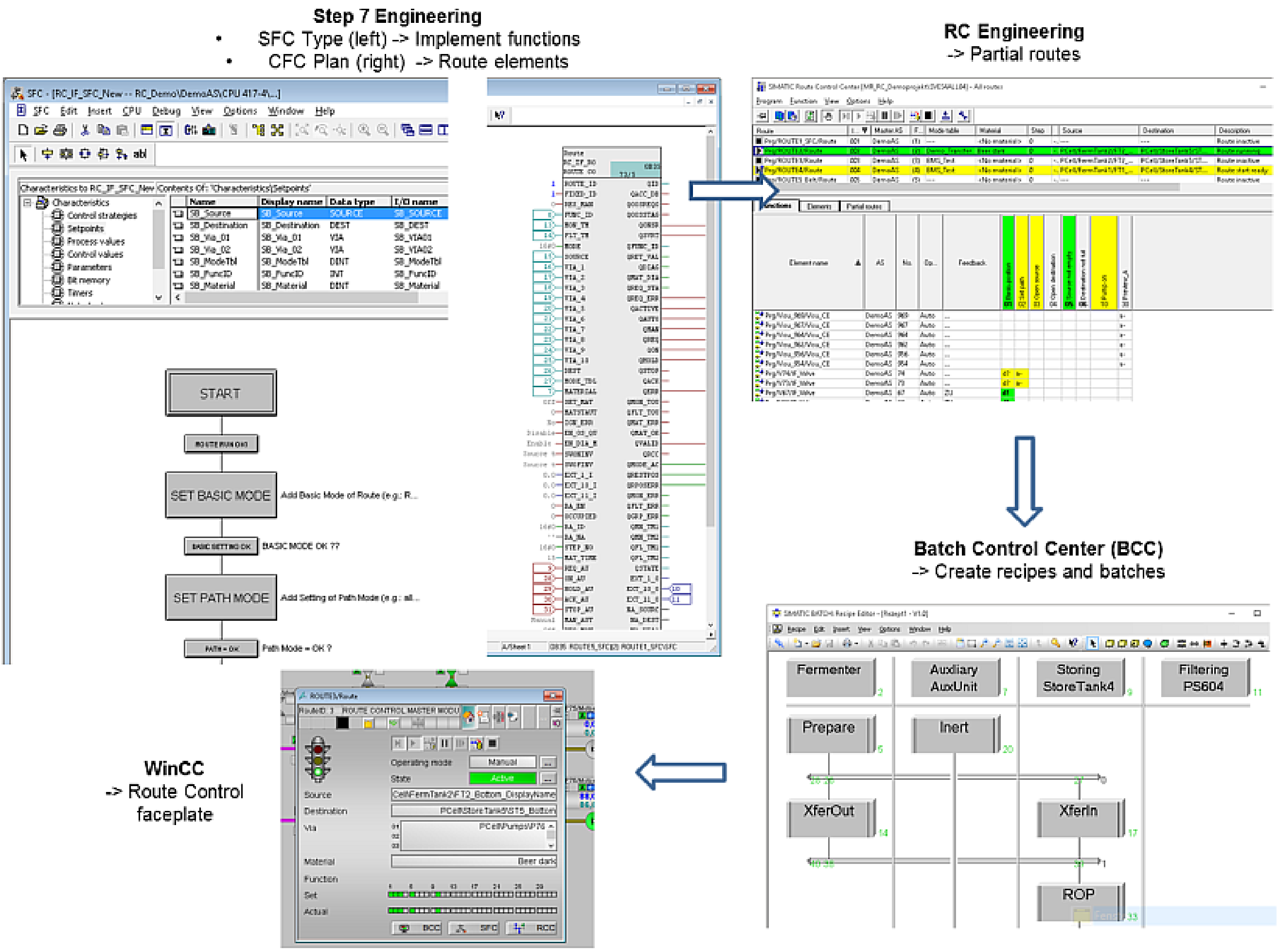
The easy-to-understand visualization in SIMATIC Route Control Center makes it easy to allocate production and cleaning paths, whereby the work involved in verification is significantly reduced. Furthermore, the material tracking is ensured by SIMATIC Route Control (Route Control Log).

Typical application examples include:

- Transport of solids and liquids
- Buffer applications and provision of buffers for production
- Bio-reactors, such as cell culture plants with upstream and downstream
- CIP and SIP procedures with various flushing paths

A Route Control server is needed in order to use SIMATIC Route Control. Route Control servers can have a redundant configuration.

SIMATIC Route Control is configured on the SIMATIC PCS 7 engineering station using the Route Control Engineering application. The following figure illustrates the individual configuring steps.



The use of SIMATIC Route Control becomes economical with as few as 5 parallel material transports. One significant benefit of this is in engineering. With the SIMATIC Route Control Engineering, routes and partial routes are created with system support.

Important functions of SIMATIC Route Control are:

- Automatic check and consideration of material compatibility (e.g. material sequences)
- Alternative transfer paths in case of malfunction (automatic)
- Status check of line
- Scaling depending on plant size
- Plant expansion without programming workload

See also

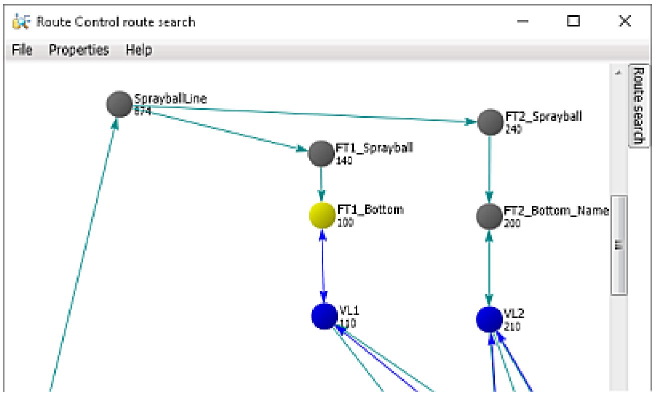
- Manual "SIMATIC PCS 7 Route Control", Online Support under entry ID 109794449 (https://support.industry.siemens.com/cs/ww/en/view/109794449)
- Product description on the Internet (https://new.siemens.com/global/en/products/automation/process-control/simatic-pcs-7/route-control.html)

Import / export

You can use the CSV interface (CSV export/import) to further simplify and accelerate configuring in SIMATIC Route Control. For example, partial routes and additional data can be edited conveniently in Excel and then imported in Route Control Engineering. The option to edit data in Excel can also be used to efficiently define routes in the specification phase and then import them.

Graphical route search

Another function is the graphical route search. This can be used to check route networks graphically.



In addition, routes can be saved and used as preferences instead of the automatic route search.

6.8 Alarm management

An alarm system must be able to perform the following basic functions:

- Warn the operator in the event of problems in the plant
- Provide information about the characteristics of the problem
- Guide the operator to the most significant problem
- Support the operator in evaluating multiple pending problems

6.8.1 Specification

The specification of an alarm system includes the following:

- Definition of formats for alarm line and alarm page
- Message classes, colors, and priorities
- Acknowledgment concept (e.g. single acknowledgment)

- Event texts, for example, "too high" for a high alarm
- Process-dependent alarm suppression, e.g. suppression of flow monitoring if a pump is switched off

These points must be defined if they deviate from standard specifications.

The preset standards for the display of message class, message color and message priority should be kept if possible and only changed at the request of the customer.

Note

If the alarm system configuration differs from the standard configuration, the differences must be documented and an update procedure described; see also chapter "System Updates and Migration (Page 169)".

See also

- Manual "PCS 7 Compendium Part A", chapter 8.1.4 "Message class, priority...", Online Support under entry ID 109809015 (https://support.industry.siemens.com/cs/ww/en/view/109809015)

6.8.2 Message classes

The different message classes, such as fault, alarm, warning, or process control message are usually defined on a function and event-specific basis. For example, if a measurement is taken, reaching the high limits will trigger an alarm, the low limits a warning, and a runtime error on a valve, for example, will trigger a fault message.

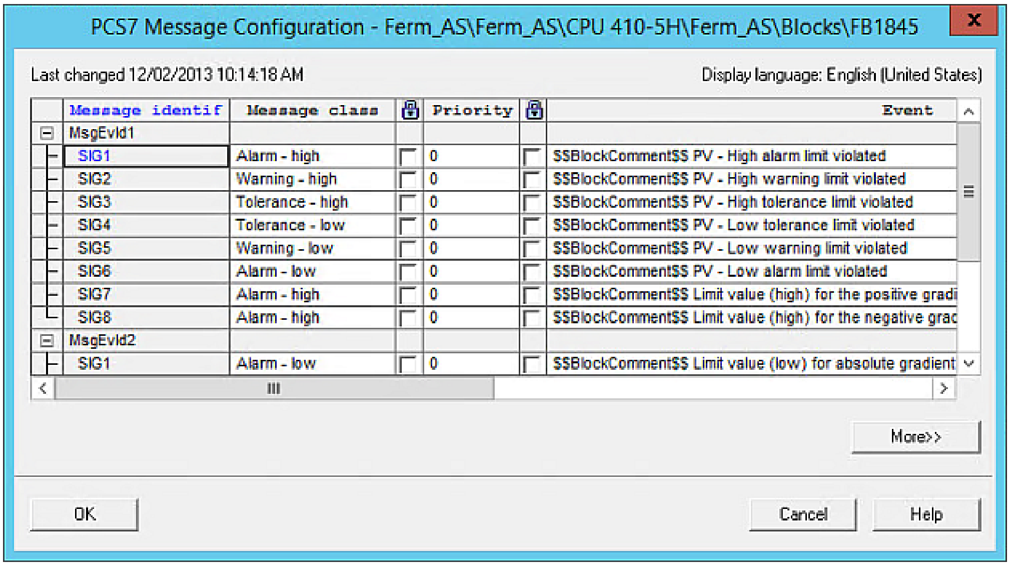
See also

- Manual "PCS 7 Compendium Part A", chapter 10.3.1 "Message classes and message types", Online Support under entry ID 109809015 (https://support.industry.siemens.com/cs/ww/en/view/109809015)

6.8.3 Priorities

To ensure that the plant operator can still perform actions even in critical situations, messages can be additionally prioritized in PCS 7 in accordance with their possible effect (plant standstill, reduction in product quality, or production delays) and the available reaction time (e.g. < 5 minutes, 5 – 20 minutes, > 20 minutes).

The priority is defined on an instance-specific basis in SIMATIC PCS 7 during message configuration and is initially set to "0". The priorities are set in the 'Messages' tab of the process object view, as shown in the following figure.



PCS7 Message Configuration - Ferm_AS\Ferm_AS\CPU 410-5H\Ferm_AS\Blocks\FB1845

Last changed 12/02/2013 10:14:18 AM

Display language: English (United States)

Message identif	Message class	🔒	Priority	🔒	Event
MsgEvId1					
SIG1	Alarm - high	□	0	□	$$BlockComment$$ PV - High alarm limit violated
SIG2	Warning - high	□	0	□	$$BlockComment$$ PV - High warning limit violated
SIG3	Tolerance - high	□	0	□	$$BlockComment$$ PV - High tolerance limit violated
SIG4	Tolerance - low	□	0	□	$$BlockComment$$ PV - Low tolerance limit violated
SIG5	Warning - low	□	0	□	$$BlockComment$$ PV - Low warning limit violated
SIG6	Alarm - low	□	0	□	$$BlockComment$$ PV - Low alarm limit violated
SIG7	Alarm - high	□	0	□	$$BlockComment$$ Limit value (high) for the positive gradi
SIG8	Alarm - high	□	0	□	$$BlockComment$$ Limit value (high) for the negative grac
MsgEvId2					
SIG1	Alarm - low	□	0	□	$$BlockComment$$ Limit value (low) for absolute gradient

Tip: The message priority can also be used to mark all GMP-relevant messages as Priority 1, for example. This will make it easier to filter for them later in the Audit Trail review.

6.8.4 Suppressing, filtering, hiding

Locking messages

When the appropriate permission is granted, in process mode the plant operator is able to set individual process tags to the "out of service" status, thus suppressing all messages of this process tag.

This function is used, for example, if a process tag is being used for the first time. The operator can use this feature to suppress messages which are of no immediate use, allowing him to focus his full attention on the relevant messages.

On all levels, operators are able to identify objects whose message reaction has been suppressed.

Filtering messages

Message filtering within alarm lists can be adapted on a user-specific basis. The filter criteria are message properties (date, time, message class, message text, etc.). The point of changing filter criteria online is to enable the user to temporarily focus on a particular period, event, etc. when analyzing errors.

Hiding messages (Smart Alarm Hiding)

This function allows alarms to be hidden on a situation-specific basis.

These messages are not taken into account when generating the collective status, i.e. the collective status of a measurement with a pending, hidden alarm does not indicate an alarm status in the process picture, is ignored when the collective-status display is generated for the diagram, and does not output an audible signal (alarm horn).

The currently pending, hidden messages can be viewed at any time in the list of hidden messages. All messages hidden by the current setting are summarized in the "Messages to be hidden" list. The messages are only hidden in terms of the display, i.e. hidden messages are still archived and taken into account during archive synchronization if a server redundancy failover is performed.

"Smart Alarm Hiding" offers two ways of hiding alarms:

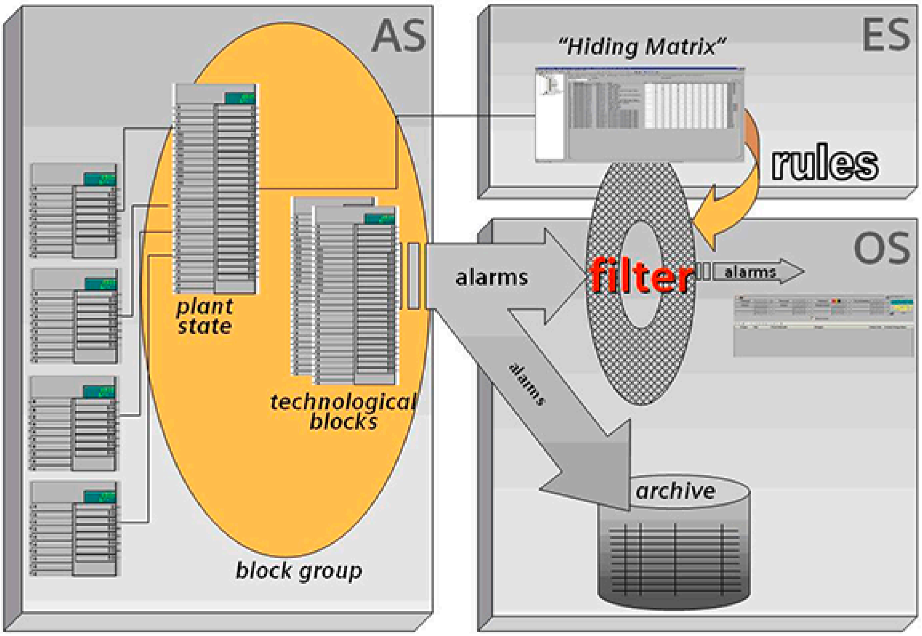
- Manual hiding and displaying of alarms
- Automatic showing and hiding of alarms, depending on process states

Hiding alarms manually:

- The alarms are shown again after a defined period of time has elapsed.
- Manually hidden alarms are acknowledged automatically.
- Manual alarm hiding applies to all clients of the relevant OS server.
- An operator message is triggered if alarms are hidden and shown manually. A reason from a drop-down list can also be specified here.

Hiding alarms automatically:

Automatic alarm hiding must be configured and is always controlled via status blocks in the AS, which hide or show state-dependent alarms in conjunction with a hiding matrix. Technological (messaging) blocks are assigned to a status block via the new "block group" block property.

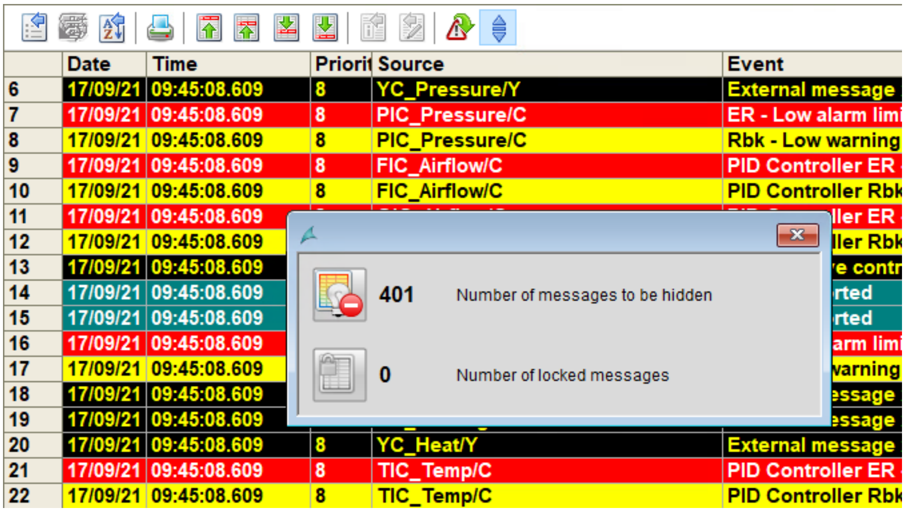


Note

The main difference between message suppression and alarm hiding is that suppressed (blocked) messages are not even generated at the respective process tag and they are therefore not sent to the OS. Neither are they recorded or archived.

Alarm hiding, on the other hand, only affects the visualization.

A symbol points out locked or hidden alarms to the operator in the overview area.



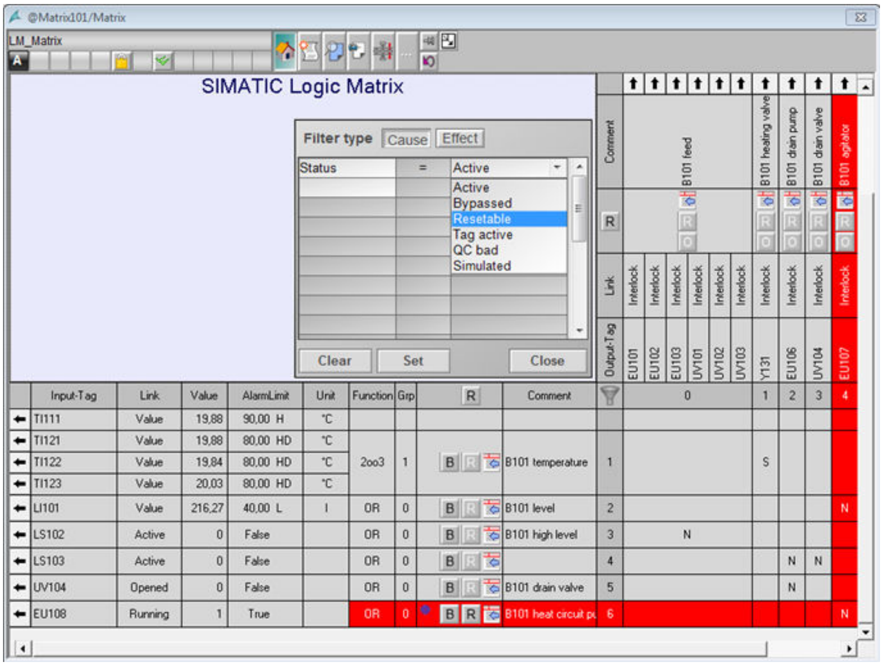
	Date	Time	Priorit	Source	Event
6	17/09/21	09:45:08.609	8	YC_Pressure/Y	External message
7	17/09/21	09:45:08.609	8	PIC_Pressure/C	ER - Low alarm limi
8	17/09/21	09:45:08.609	8	PIC_Pressure/C	Rbk - Low warning
9	17/09/21	09:45:08.609	8	FIC_Airflow/C	PID Controller ER
10	17/09/21	09:45:08.609	8	FIC_Airflow/C	PID Controller Rbk
11	17/09/21	09:45:08.609			ller ER
12	17/09/21	09:45:08.609			ller Rbk
13	17/09/21	09:45:08.609			e contr
14	17/09/21	09:45:08.609			rted
15	17/09/21	09:45:08.609			rted
16	17/09/21	09:45:08.609			arm limi
17	17/09/21	09:45:08.609			warning
18	17/09/21	09:45:08.609			essage
19	17/09/21	09:45:08.609			essage
20	17/09/21	09:45:08.609	8	YC_Heat/Y	External message
21	17/09/21	09:45:08.609	8	TIC_Temp/C	PID Controller ER
22	17/09/21	09:45:08.609	8	TIC_Temp/C	PID Controller Rbk

401 Number of messages to be hidden

0 Number of locked messages

6.8.5 SIMATIC PCS 7 Logic Matrix

The SIMATIC Logic Matrix simplifies the configuring of safety interlocking. The direct advantage is the clear arrangement of the matrix, which makes errors during configuration less likely for one thing. For another, it facilitates the checking of the code and thus also the validation.



Output-Tag	Link	Comment	Grp
EU101	Interlock	B101 feed	0
EU102	Interlock		
EU103	Interlock		
UV101	Interlock		
UV102	Interlock		
UV103	Interlock		
Y131	Interlock	B101 heating valve	1
EU106	Interlock	B101 drain pump	2
UV104	Interlock	B101 drain valve	3
EU107	Interlock	B101 agitator	4

Input-Tag	Link	Value	AlarmLimit	Unit	Function	Grp	Comment		0	1	2	3	4
TI111	Value	19,88	90,00 H	°C									
TI121	Value	19,88	80,00 HD	°C	2oo3	1	B101 temperature	1		S			
TI122	Value	19,84	80,00 HD	°C									
TI123	Value	20,03	80,00 HD	°C									
LI101	Value	216,27	40,00 L	l	OR	0	B101 level	2					N
LS102	Active	0	False		OR	0	B101 high level	3	N				
LS103	Active	0	False		OR	0		4			N	N	
UV104	Opened	0	False		OR	0	B101 drain valve	5			N		
EU108	Running	1	True		OR	0	B101 heat circuit pu	6					N

The figure shows the user interface of the SIMATIC Logic Matrix on the operator station. The inputs are shown on the bottom left and the outputs on the top right. The cause and effect are apparent at a glance.

See also

- Manual "SIMATIC PCS 7 Logic Matrix", Online Support under entry ID 109794041 (https://support.industry.siemens.com/cs/ww/en/view/109794041)

6.8.6 Monitoring PCS 7 components – Lifebeat monitoring

SIMATIC PCS 7 Lifebeat Monitoring allows the functionality of automation and operator stations to be monitored. To facilitate this, all automation and operator stations must be configured in HW Config and the OPC connections to the operator stations must be created.

To configure the nodes to be monitored in WinCC Explorer, select the menu command *Editor > Lifebeat monitoring > Open*. Here, all the nodes to be monitored and the monitoring cycle in which lifebeat monitoring will be performed can be configured. A control system message is triggered as soon as a configured station does not respond to the monitoring request.

The lifebeat monitoring is activated automatically when the OS starts up.

See also

- Manual "PCS 7 Operator Station", Online Support under entry ID 109794374 (https://support.industry.siemens.com/cs/ww/en/view/109794374)

Note

Alternatively, all process control equipment can also be managed in the PCS 7 Asset Management. Asset management does not require any additional configuration, see also chapter "Asset Management (Page 165)". A maintenance station provides an overview of the diagnostic and service information for all equipment. However, lifebeat monitoring of a plant with a maintenance station is not permitted.

6.8.7 Monitoring PCS 7 components – SMMC

The SIMATIC Management Console (SMMC) is a program package, which supports the monitoring, documentation and management of the hardware and software installed. To use the SMMC, the software package is to be installed on a PC. In doing so, either a separate computer or the existing ES should be used. The "SIMATIC Management Agent" is also to be installed on computers to be managed.

The SMMC can now be used to created detailed reports on the currently installed hardware and software. The data required for this purpose is taken directly by the SMMC from computers and AS systems of the plant. The documentation always corresponds to the actual "As Built" state of the plant.

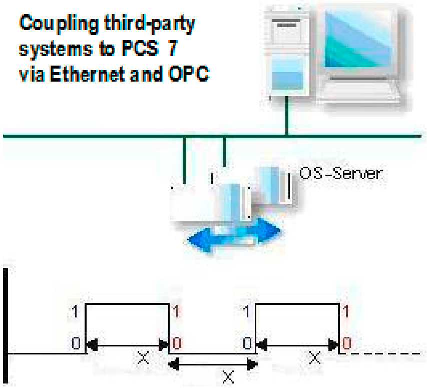
The permissions for the SIMATIC Management Console must be set up separately.

See also

- Manual "SIMATIC Management Console", chapter 4.1, Online Support under entry ID 109794443 (https://support.industry.siemens.com/cs/ww/en/view/109794443)

6.8.8 Monitoring connected systems

Lifebeat monitoring for connected systems must be configured manually. Its use depends on the corresponding communication partner. If the connected system represents an important interface to SIMATIC PCS 7, lifebeat monitoring is absolutely necessary.



The graphic shows an example of a solution for lifebeat monitoring with a third-party system. SIMATIC PCS 7 sets a defined OPC variable bit from logic 0 to 1. After a defined period of time X, the connected system must reset the OPC variable bit from logic 1 to 0.

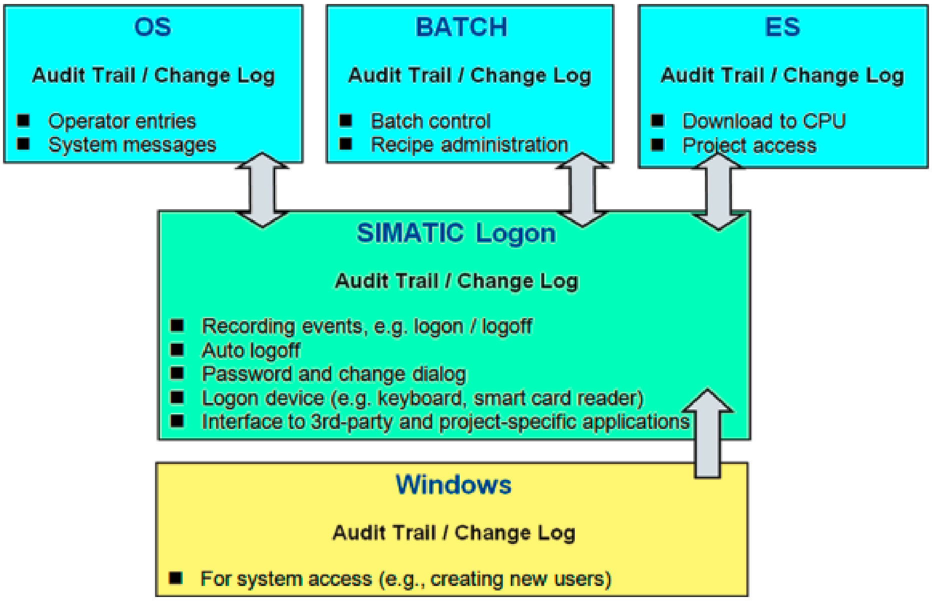
This operation is repeated in cycles. If the connected system does not perform a state transition within the specified time, a process control message is generated in the SIMATIC PCS 7 process control system. This message indicates to the operator that communication with the connected system is not functioning correctly.

6.9 Audit trail and change control

Traceability of operator intervention and critical parameters and data changes must be recorded with information about the operator (audit trail). The requirements of this topic are defined by 21 CFR Part 11 of the U.S. Food and Drug Administration, for example.

In a controlled environment, changes to the project configuration or user management, for example, are subject to change control. This change control is supported by recording log files.

In a PCS 7 system, this is implemented by a multilayered approach to the topics of Audit Trail and change control.



6.9.1 PCS 7 ES

Online changes on the PCS 7 ES

Typically, configuration data on the engineering level is not directly subject to the extremely strict requirements of 21 CFR Part 11. Having said that, system components are usually concerned, which must be validated and controlled.

The traceable online parameter change feature also enables certain quality-related data to be accessed directly via the ES. However, it is practical and advisable in a regulated environment for such interventions to only be performed on the operator control level and with the corresponding operator permission. Such changes are then being recorded in the central audit trail of the OS.

Note

Parameter changes made on the OS interface are not automatically transferred to the offline project. To do this, the relevant parameters must be selected and the "Read back parameters" function executed.

Depending on the customer, controlled online parameter changes made via the ES may sometimes be accepted, or even desired, during the commissioning phase. However, once a plant has been validated, such parameter changes must be made exclusively via the OS level or on the ES by means of a change request.

See also

- FAQ "Labeling parameters for read-back", Online Support under entry ID 23967880 (https://support.industry.siemens.com/cs/ww/en/view/23967880)

Change control of the ES / AS configuration

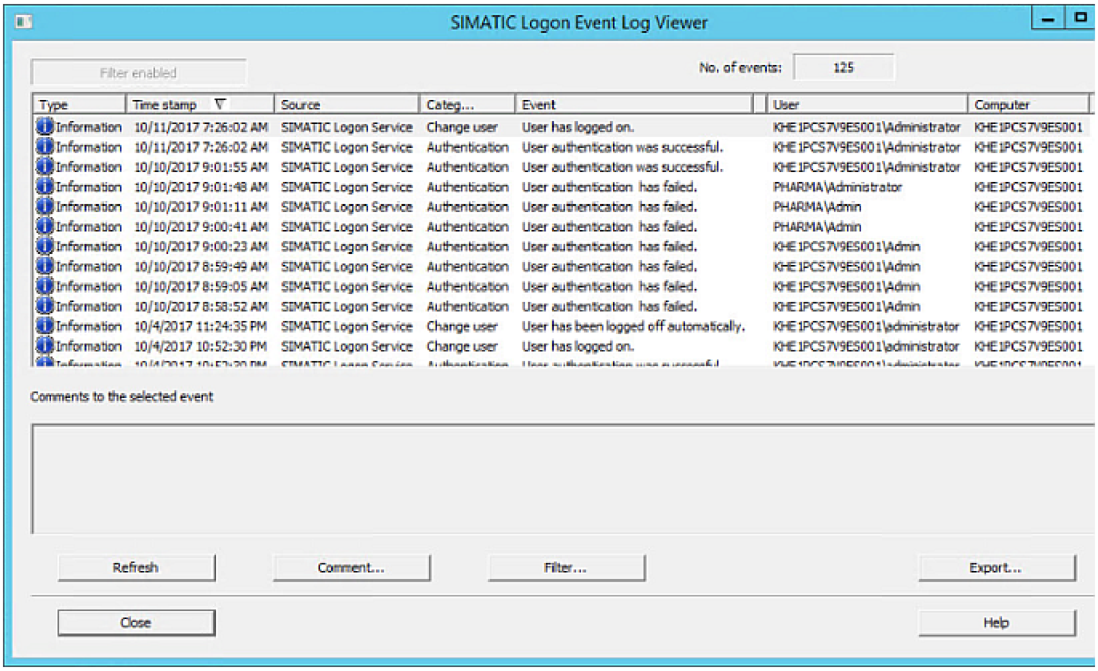
Various tools are suitable for controlling the offline configuration in the ES, when used in conjunction with a defined change process and an appropriate strategy for backing up project data. The Version Cross Manager, for example, enables users to compare different project versions with each other; see chapter "Version comparison with Version Cross Manager (VXM) (Page 152)".

The current status of the offline/online configuration can also be verified by activating "test mode" in the ES. Parameter readback also has to be taken into account here, see "Note" above.

Project access activities and online changes performed on the ES are recorded with the aid of the SIMATIC Logon change log, in a similar way to an audit trail (who has changed what and when). The following are logged:

- Events relating to access protection (open project, access to project denied, activate/deactivate access protection, etc.)
- Target system events (AS configuration loaded, software application loaded, online mode activated/deactivated)

- Events relating to online value changes (old value, new value)
- Version changes (archiving of versioned projects)



SIMATIC Logon Event Log Viewer

Filter enabled

No. of events: 125

Type	Time stamp	Source	Categ...	Event	User	Computer
Information	10/11/2017 7:26:02 AM	SIMATIC Logon Service	Change user	User has logged on.	KHE1PCS7V9ES001\Administrator	KHE1PCS7V9ES001
Information	10/11/2017 7:26:02 AM	SIMATIC Logon Service	Authentication	User authentication was successful.	KHE1PCS7V9ES001\Administrator	KHE1PCS7V9ES001
Information	10/10/2017 9:01:55 AM	SIMATIC Logon Service	Authentication	User authentication was successful.	KHE1PCS7V9ES001\Administrator	KHE1PCS7V9ES001
Information	10/10/2017 9:01:48 AM	SIMATIC Logon Service	Authentication	User authentication has failed.	PHARMA\Administrator	KHE1PCS7V9ES001
Information	10/10/2017 9:01:11 AM	SIMATIC Logon Service	Authentication	User authentication has failed.	PHARMA\Admin	KHE1PCS7V9ES001
Information	10/10/2017 9:00:41 AM	SIMATIC Logon Service	Authentication	User authentication has failed.	PHARMA\Admin	KHE1PCS7V9ES001
Information	10/10/2017 9:00:23 AM	SIMATIC Logon Service	Authentication	User authentication has failed.	KHE1PCS7V9ES001\Admin	KHE1PCS7V9ES001
Information	10/10/2017 8:59:49 AM	SIMATIC Logon Service	Authentication	User authentication has failed.	KHE1PCS7V9ES001\Admin	KHE1PCS7V9ES001
Information	10/10/2017 8:59:05 AM	SIMATIC Logon Service	Authentication	User authentication has failed.	KHE1PCS7V9ES001\Admin	KHE1PCS7V9ES001
Information	10/10/2017 8:58:52 AM	SIMATIC Logon Service	Authentication	User authentication has failed.	KHE1PCS7V9ES001\Admin	KHE1PCS7V9ES001
Information	10/4/2017 11:24:35 PM	SIMATIC Logon Service	Change user	User has been logged off automatically.	KHE1PCS7V9ES001\administrator	KHE1PCS7V9ES001
Information	10/4/2017 10:52:30 PM	SIMATIC Logon Service	Change user	User has logged on.	KHE1PCS7V9ES001\administrator	KHE1PCS7V9ES001
Information	10/4/2017 10:52:30 PM	SIMATIC Logon Service	Authentication	User authentication was successful.	KHE1PCS7V9ES001\administrator	KHE1PCS7V9ES001

Comments to the selected event

Change control for AS download

In addition to protection against unauthorized access to the ES configuration via the "Activate Access Protection" project setting, a CPU password can also be used to protect against unauthorized downloads to the CPU.

However, as with online value changes, downloads made to the CPU are not recorded unless the change log file is activated, see chapter "PCS 7 ES" above regarding ES change control.

Note

The time at which this access protection should be activated and the activation of the change log file must be defined together with the customer at an early stage. Depending on the configuration environment, it may be practical to have access protection in place even as early as the configuration phase, with the change log file being activated at the start of the FAT.

Once access protection is configured, you can often forgo the additional CPU password, if the customer agrees to it.

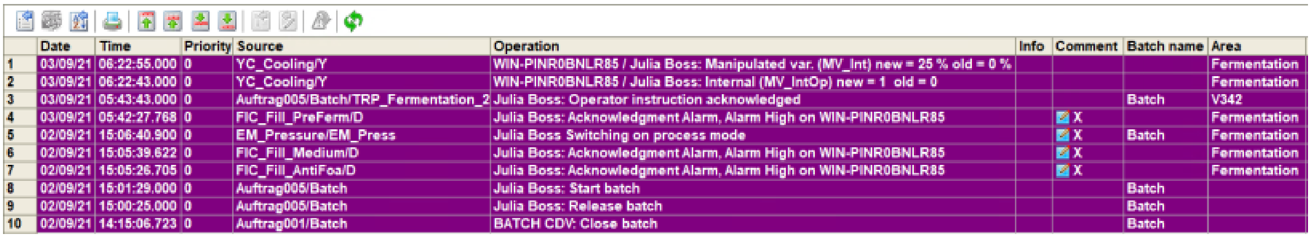
6.9.2 PCS 7 OS

Audit trail in PCS 7 OS

SIMATIC PCS 7 records all operations and parameter changes performed in process mode, assigning them to the "Operating messages" message class in the message archive. If parameter changes are made via input/output fields, the output of a message must be configured separately.

Acknowledgments of alarms, warnings, system messages, etc. are available in the "history" of the process control system. Message acknowledgements can be provided with a mandatory comment.

The figure below shows an extract taken from the operation list.



	Date	Time	Priority	Source	Operation	Info	Comment	Batch name	Area
1	03/09/21	06:22:55.000	0	YC_Cooling/Y	WIN-PINR0BNLR85 / Julia Boss: Manipulated var. (MV_Int) new = 25 % old = 0 %				Fermentation
2	03/09/21	06:22:43.000	0	YC_Cooling/Y	WIN-PINR0BNLR85 / Julia Boss: Internal (MV_IntOp) new = 1 old = 0				Fermentation
3	03/09/21	05:43:43.000	0	Auftrag005/Batch/TRP_Fermentation_2	Julia Boss: Operator instruction acknowledged			Batch	V342
4	03/09/21	05:42:27.768	0	FIC_Fill_PreFerm/D	Julia Boss: Acknowledgment Alarm, Alarm High on WIN-PINR0BNLR85		✎ X		Fermentation
5	02/09/21	15:06:40.900	0	EM_Pressure/EM_Press	Julia Boss Switching on process mode		✎ X	Batch	Fermentation
6	02/09/21	15:05:39.622	0	FIC_Fill_Medium/D	Julia Boss: Acknowledgment Alarm, Alarm High on WIN-PINR0BNLR85		✎ X		Fermentation
7	02/09/21	15:05:26.705	0	FIC_Fill_AntiFoa/D	Julia Boss: Acknowledgment Alarm, Alarm High on WIN-PINR0BNLR85		✎ X		Fermentation
8	02/09/21	15:01:29.000	0	Auftrag005/Batch	Julia Boss: Start batch			Batch	
9	02/09/21	15:00:25.000	0	Auftrag005/Batch	Julia Boss: Release batch			Batch	
10	02/09/21	14:15:06.723	0	Auftrag001/Batch	BATCH CDV: Close batch			Batch	

Note

Select the hard disk capacity so that the entire alarm log can be securely stored there until it is exported to an external data medium.

The actual audit trail required by law only contains the changes to GMP-relevant values. It is, therefore, an excerpt of the recorded operations. These can be filtered, for example, using a separate message priority, see also chapter "Priorities (Page 107)". As an alternative, the relevant operating messages can also be realized with an add-on, see chapter "OPD – User dialogs and electronic signatures (Page 39)".

Note

In a distributed system, a standard server must be assigned to the OS client so that messages and alarms can be transferred correctly. You can find an explanation in the Manual "PCS 7 Compendium Part A".

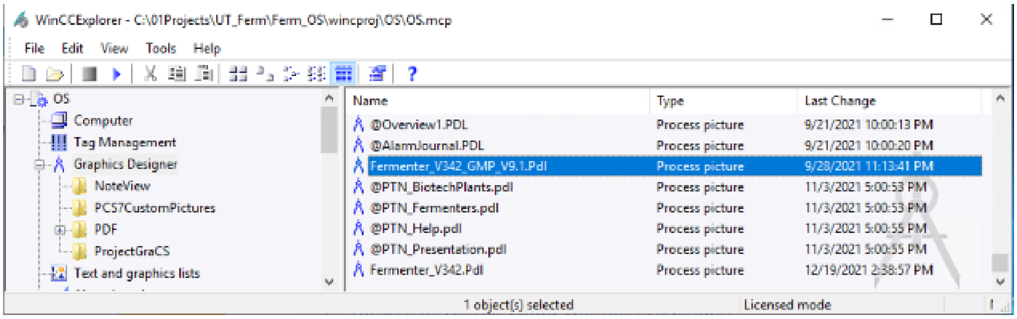
See also

- Manual "PCS 7 Compendium Part A", chapter 10.1.3 "Selecting and configuring a standard server", Online Support under entry ID 109809015 (https://support.industry.siemens.com/cs/ww/en/view/109809015)

Change control of the OS configuration

The OS configuration, as well as the project engineering of OS elements (pictures, scripts, etc.), is versioned on the ES (SIMATIC Version Trail) and archived, together with the overall project. The changes that were made can be documented using a screenshot and the screenshot appended to the change request.

Changed operating screens can be identified using the date of change in the component view of the SIMATIC Manager. Operating screens can also be protected from modification via the WinCC Explorer with a password, see chapter "Protection of graphics (Page 157)".



Name	Type	Last Change
@Overview1.PDL	Process picture	9/21/2021 10:00:13 PM
@AlarmJournal.PDL	Process picture	9/21/2021 10:00:20 PM
Fermenter_V342_GMP_V9.1.Pdl	Process picture	9/28/2021 11:13:41 PM
@PTN_BiotechPlants.pdl	Process picture	11/3/2021 5:00:53 PM
@PTN_Fermenters.pdl	Process picture	11/3/2021 5:00:53 PM
@PTN_Help.pdl	Process picture	11/3/2021 5:00:55 PM
@PTN_Presentation.pdl	Process picture	11/3/2021 5:00:55 PM
Fermenter_V342.Pdl	Process picture	12/19/2021 2:38:57 PM

1 object(s) selected   Licensed mode

If you want to track changes to graphics automatically and in detail, you can do this by using an add-on, see chapter "versiondog – Version assignment and configuration control (Page 38)".

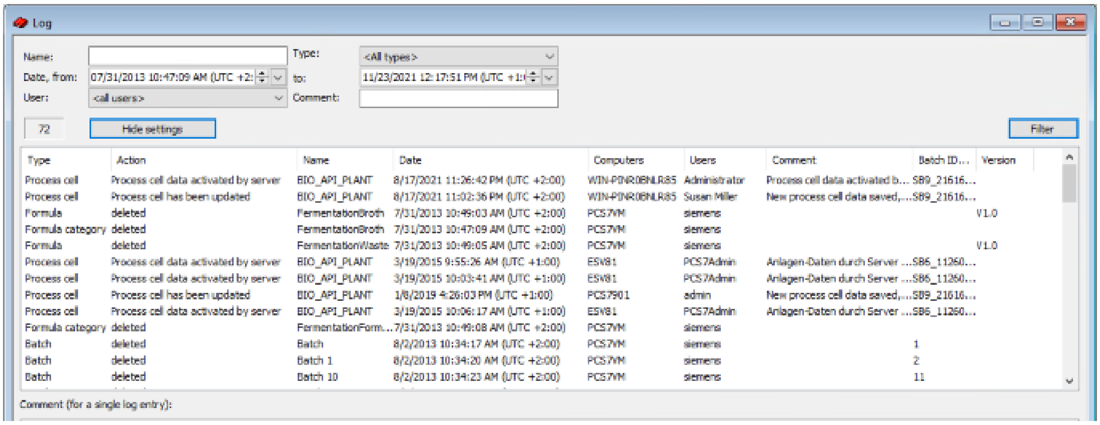
Changes made to individual OS elements and other changes must be controlled in accordance with the applicable change procedure following their initial approval. The tools used for documenting the changes only offer support.

6.9.3 SIMATIC BATCH

Audit trail in SIMATIC BATCH

Operator actions performed in SIMATIC BATCH are recorded in the same message archive as OS operator actions (see above).

In addition, the user actions you perform in BatchCC are recorded in the SIMATIC BATCH log.

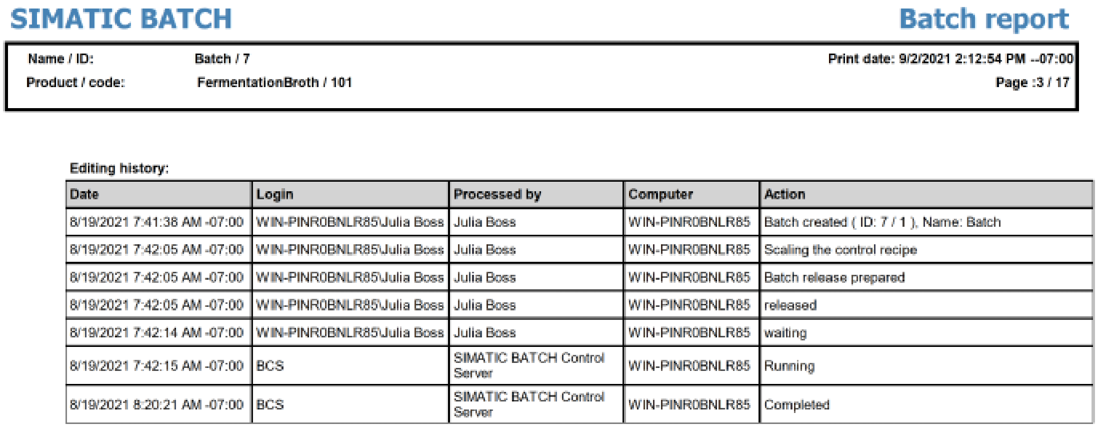


Name:
Type: <All types>
Date, from: 07/31/2013 10:47:09 AM (UTC +2:
to: 11/23/2021 12:17:51 PM (UTC +1:
User: <all users>
Comment:
72

Type	Action	Name	Date	Computers	Users	Comment	Batch ID...	Version
Process cell	Process cell data activated by server	BIO_API_PLANT	8/17/2021 11:26:42 PM (UTC +2:00)	WIN-PINR0BNLR85	Administrator	Process cell data activated b...	SB9_21616...	
Process cell	Process cell has been updated	BIO_API_PLANT	8/17/2021 11:02:36 PM (UTC +2:00)	WIN-PINR0BNLR85	Susan Miller	New process cell data saved,...	SB9_21616...	
Formula	deleted	FermentationBroth	7/31/2013 10:49:03 AM (UTC +2:00)	PCS7VM	siemens			V1.0
Formula category	deleted	FermentationBroth	7/31/2013 10:47:09 AM (UTC +2:00)	PCS7VM	siemens			
Formula	deleted	FermentationWaste	7/31/2013 10:49:05 AM (UTC +2:00)	PCS7VM	siemens			V1.0
Process cell	Process cell data activated by server	BIO_API_PLANT	3/19/2015 9:55:26 AM (UTC +1:00)	ESV81	PCS7Admin	Anlagen-Daten durch Server ...	SB6_11260...	
Process cell	Process cell data activated by server	BIO_API_PLANT	3/19/2015 10:03:41 AM (UTC +1:00)	ESV81	PCS7Admin	Anlagen-Daten durch Server ...	SB6_11260...	
Process cell	Process cell has been updated	BIO_API_PLANT	1/8/2019 4:26:03 PM (UTC +1:00)	PCS7901	admin	New process cell data saved,...	SB9_21616...	
Process cell	Process cell data activated by server	BIO_API_PLANT	3/19/2015 10:06:17 AM (UTC +1:00)	ESV81	PCS7Admin	Anlagen-Daten durch Server ...	SB6_11260...	
Formula category	deleted	FermentationForm...	7/31/2013 10:49:08 AM (UTC +2:00)	PCS7VM	siemens			
Batch	deleted	Batch	8/2/2013 10:34:17 AM (UTC +2:00)	PCS7VM	siemens		1	
Batch	deleted	Batch 1	8/2/2013 10:34:20 AM (UTC +2:00)	PCS7VM	siemens		2	
Batch	deleted	Batch 10	8/2/2013 10:34:23 AM (UTC +2:00)	PCS7VM	siemens		11	

Comment (for a single log entry):

A batch report containing information on the operator actions performed for each batch (who, when, what) is also created in SIMATIC BATCH.



SIMATIC BATCH

Batch report

Name / ID: Batch / 7

Product / code: FermentationBroth / 101

Print date: 9/2/2021 2:12:54 PM --07:00

Page :3 / 17

Editing history:

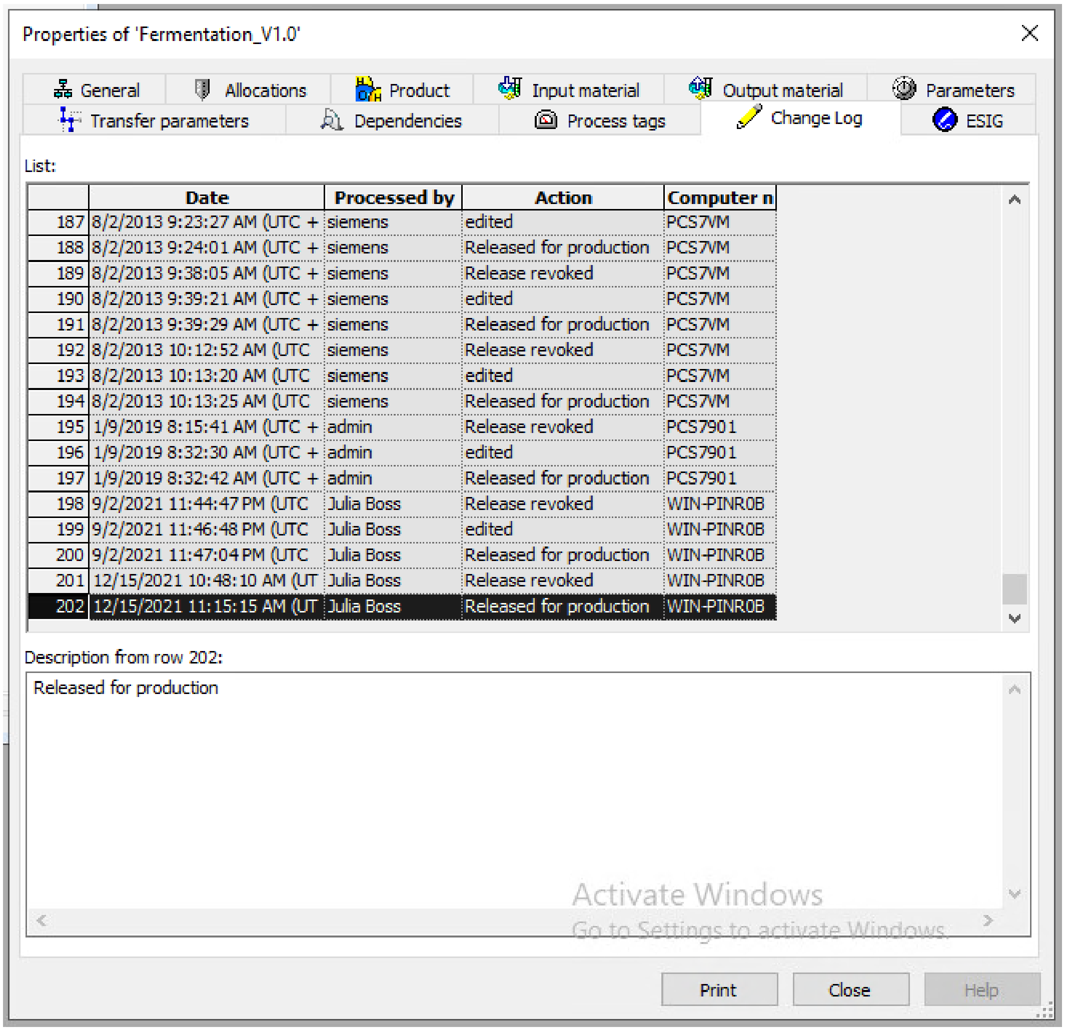
Date	Login	Processed by	Computer	Action
8/19/2021 7:41:38 AM -07:00	WIN-PINR0BNLR85\Julia Boss	Julia Boss	WIN-PINR0BNLR85	Batch created (ID: 7 / 1), Name: Batch
8/19/2021 7:42:05 AM -07:00	WIN-PINR0BNLR85\Julia Boss	Julia Boss	WIN-PINR0BNLR85	Scaling the control recipe
8/19/2021 7:42:05 AM -07:00	WIN-PINR0BNLR85\Julia Boss	Julia Boss	WIN-PINR0BNLR85	Batch release prepared
8/19/2021 7:42:05 AM -07:00	WIN-PINR0BNLR85\Julia Boss	Julia Boss	WIN-PINR0BNLR85	released
8/19/2021 7:42:14 AM -07:00	WIN-PINR0BNLR85\Julia Boss	Julia Boss	WIN-PINR0BNLR85	waiting
8/19/2021 7:42:15 AM -07:00	BCS	SIMATIC BATCH Control Server	WIN-PINR0BNLR85	Running
8/19/2021 8:20:21 AM -07:00	BCS	SIMATIC BATCH Control Server	WIN-PINR0BNLR85	Completed

Change control for recipes and batch objects

The change control for recipes is supported by:

- Change log for essential processing steps
- Version assignment and release workflow including signatures
- Authorizations and project settings
- Recipe comparer

The changes to recipes, formulas, libraries, batches and materials are documented in the **change log**. The user, the time of day and the action are entered.



List:

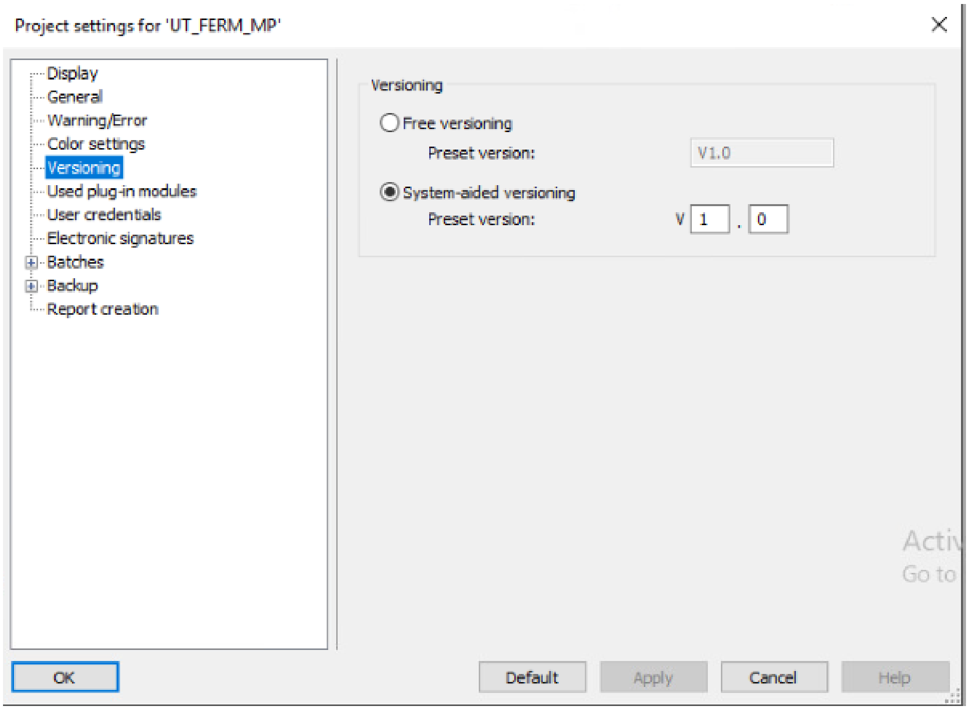
	Date	Processed by	Action	Computer n
187	8/2/2013 9:23:27 AM (UTC +	siemens	edited	PCS7VM
188	8/2/2013 9:24:01 AM (UTC +	siemens	Released for production	PCS7VM
189	8/2/2013 9:38:05 AM (UTC +	siemens	Release revoked	PCS7VM
190	8/2/2013 9:39:21 AM (UTC +	siemens	edited	PCS7VM
191	8/2/2013 9:39:29 AM (UTC +	siemens	Released for production	PCS7VM
192	8/2/2013 10:12:52 AM (UTC	siemens	Release revoked	PCS7VM
193	8/2/2013 10:13:20 AM (UTC	siemens	edited	PCS7VM
194	8/2/2013 10:13:25 AM (UTC	siemens	Released for production	PCS7VM
195	1/9/2019 8:15:41 AM (UTC +	admin	Release revoked	PCS7901
196	1/9/2019 8:32:30 AM (UTC +	admin	edited	PCS7901
197	1/9/2019 8:32:42 AM (UTC +	admin	Released for production	PCS7901
198	9/2/2021 11:44:47 PM (UTC	Julia Boss	Release revoked	WIN-PINR0B
199	9/2/2021 11:46:48 PM (UTC	Julia Boss	edited	WIN-PINR0B
200	9/2/2021 11:47:04 PM (UTC	Julia Boss	Released for production	WIN-PINR0B
201	12/15/2021 10:48:10 AM (UT	Julia Boss	Release revoked	WIN-PINR0B
202	12/15/2021 11:15:15 AM (UT	Julia Boss	Released for production	WIN-PINR0B

Description from row 202:

Released for production

To ensure consistent **version management**, the following project settings must be made:

- "System-aided versioning" option is selected



Project settings for 'UT_FERM_MP'

Versioning

○ Free versioning

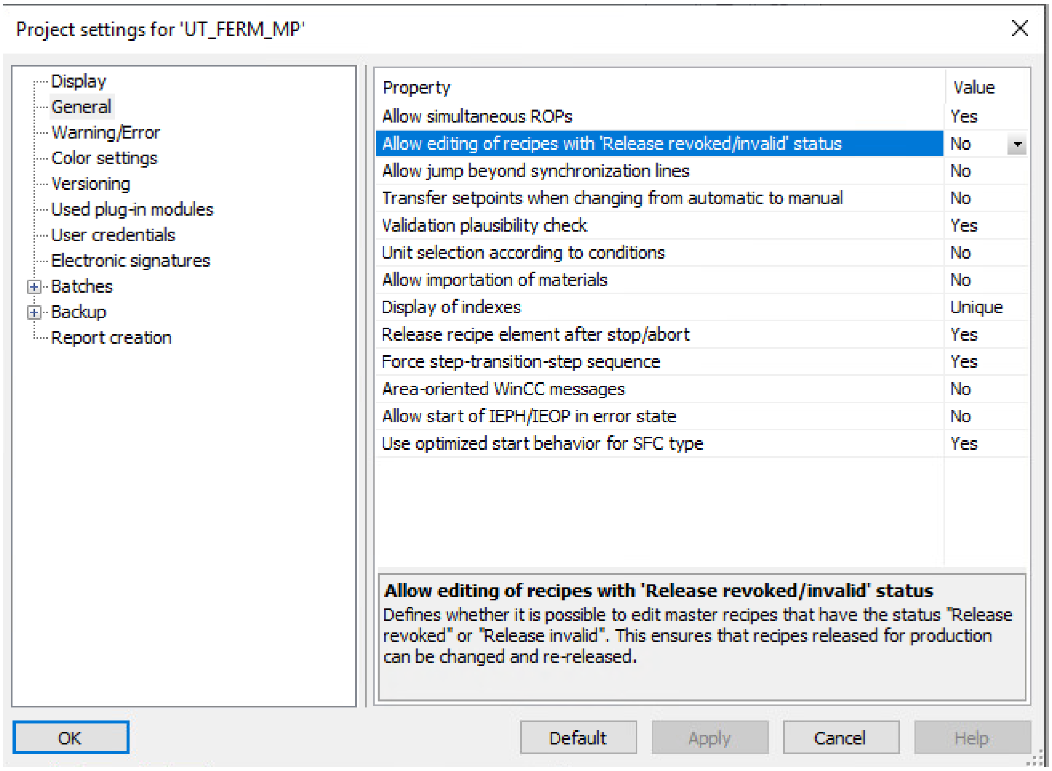
Preset version: V1.0

● System-aided versioning

Preset version: V 1 . 0

and

- The property "Allow editing of recipes with 'Release revoked/invalid' status" is **deactivated** (default is "yes").

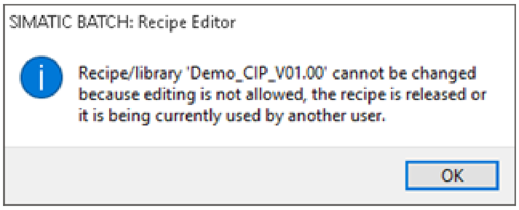


Property	Value
Allow simultaneous ROPs	Yes
Allow editing of recipes with 'Release revoked/invalid' status	No
Allow jump beyond synchronization lines	No
Transfer setpoints when changing from automatic to manual	No
Validation plausibility check	Yes
Unit selection according to conditions	No
Allow importation of materials	No
Display of indexes	Unique
Release recipe element after stop/abort	Yes
Force step-transition-step sequence	Yes
Area-oriented WinCC messages	No
Allow start of IEPH/IEOP in error state	No
Use optimized start behavior for SFC type	Yes

Allow editing of recipes with 'Release revoked/invalid' status
Defines whether it is possible to edit master recipes that have the status "Release revoked" or "Release invalid". This ensures that recipes released for production can be changed and re-released.

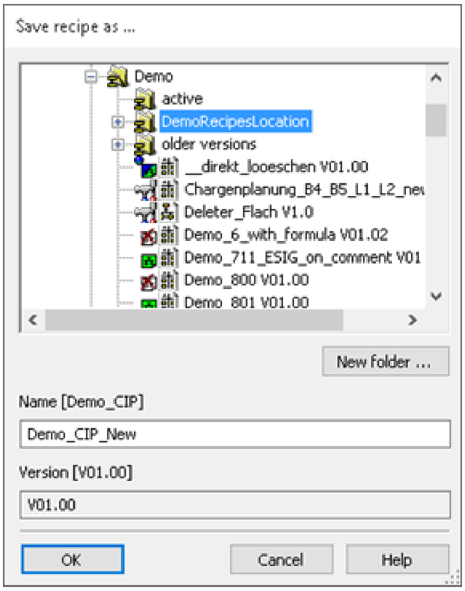
If these settings are made, the message below is output if a change is to be made to a recipe.

The recipe can only be edited after "Save As" has been used:



Recipe/library 'Demo_CIP_V01.00' cannot be changed because editing is not allowed, the recipe is released or it is being currently used by another user.

->



Name [Demo_CIP]: Demo_CIP_New

Version [V01.00]: V01.00

Note

The above setting ensures that once a recipe is released, it cannot be edited later without changing the version or name.

The **Comparison of recipe objects** in the BatchCC enables a comparison of various versions of master recipes, libraries and formulas.

See also

- FAQ "Saving recipes", Online Support under entry ID 23378328 (https://support.industry.siemens.com/cs/ww/en/view/23378328)
- Manual "SIMATIC BATCH", chapter 15.1.2.5 "Versioning" and chapter 9.5.9 "Comparing recipe objects", Online Support under entry ID 109794450 (https://support.industry.siemens.com/cs/ww/en/view/109794450)

6.10 Configuration for electronic signatures

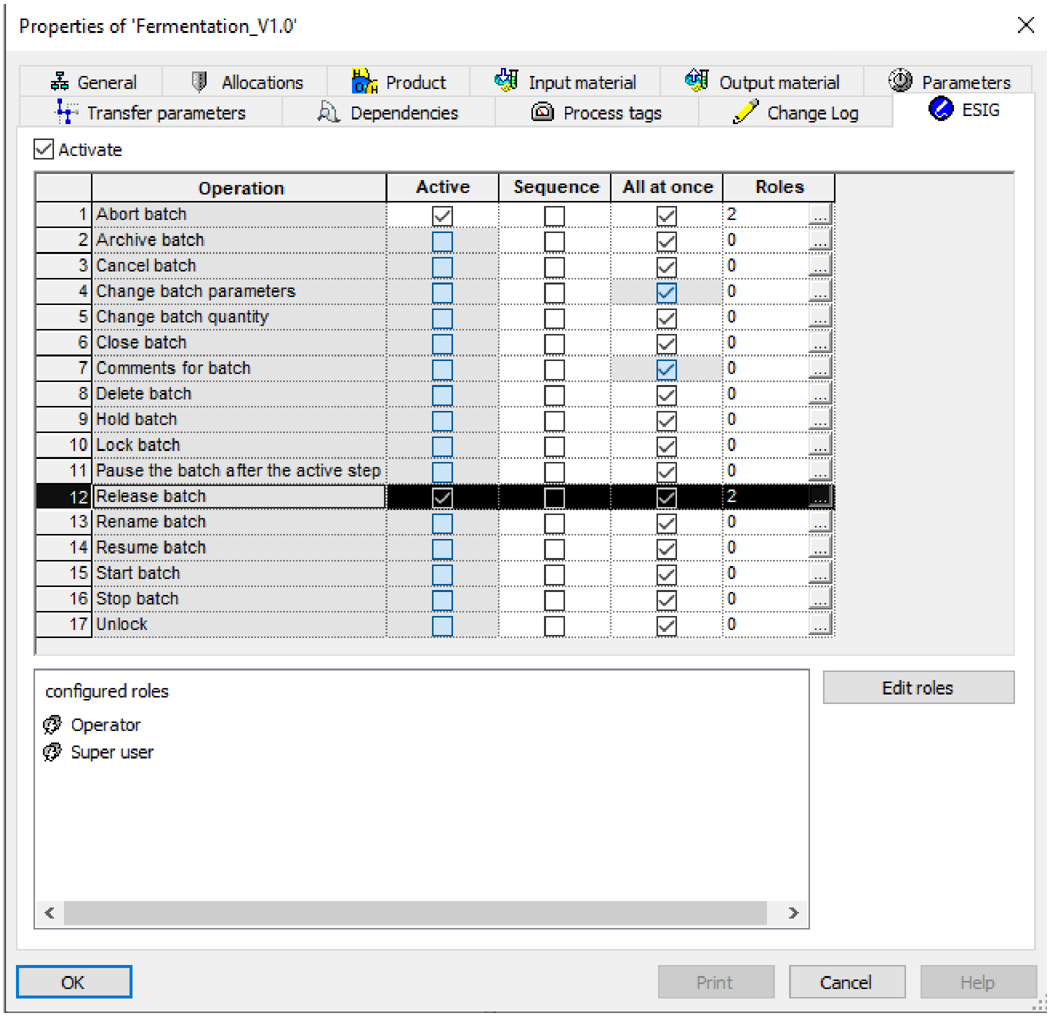
If electronic signatures are to be used in a computer system instead of handwritten signatures, compliance is required for certain legal regulations, such as those contained in 21 CFR Part 11 of the U.S. Food and Drug Administration or also Annex 11 of the EU GMP Guide.

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

6.10.1 Electronic signature in SIMATIC BATCH

With the installation of SIMATIC Logon, an "Electronic Signature" package will also be available, whose basic function is to enable electronic signatures to be used in SIMATIC BATCH. The figure below shows the "Properties" dialog window for configuring electronic signatures.

Two electronic signatures are required in this example; They are specified in the SIMATIC BATCH Recipe Editor in the "Configured roles" box.



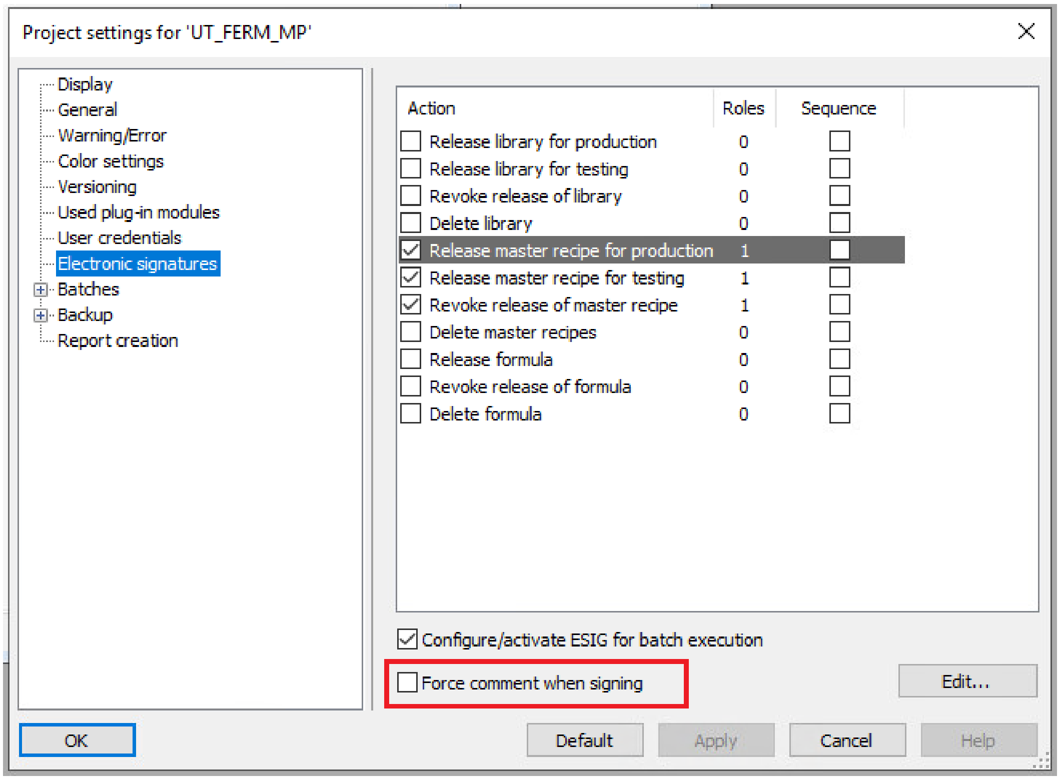
Properties of 'Fermentation_V1.0'

☑ Activate

	Operation	Active	Sequence	All at once	Roles
1	Abort batch	☑	□	☑	2
2	Archive batch	□	□	☑	0
3	Cancel batch	□	□	☑	0
4	Change batch parameters	□	□	☑	0
5	Change batch quantity	□	□	☑	0
6	Close batch	□	□	☑	0
7	Comments for batch	□	□	☑	0
8	Delete batch	□	□	☑	0
9	Hold batch	□	□	☑	0
10	Lock batch	□	□	☑	0
11	Pause the batch after the active step	□	□	☑	0
12	Release batch	☑	□	☑	2
13	Rename batch	□	□	☑	0
14	Resume batch	□	□	☑	0
15	Start batch	□	□	☑	0
16	Stop batch	□	□	☑	0
17	Unlock	□	□	☑	0

configured roles
Operator
Super user

The project settings can also be used to make an electronic signature necessary for releasing recipes, parameter sets (formulas), and recipe operations, for example.

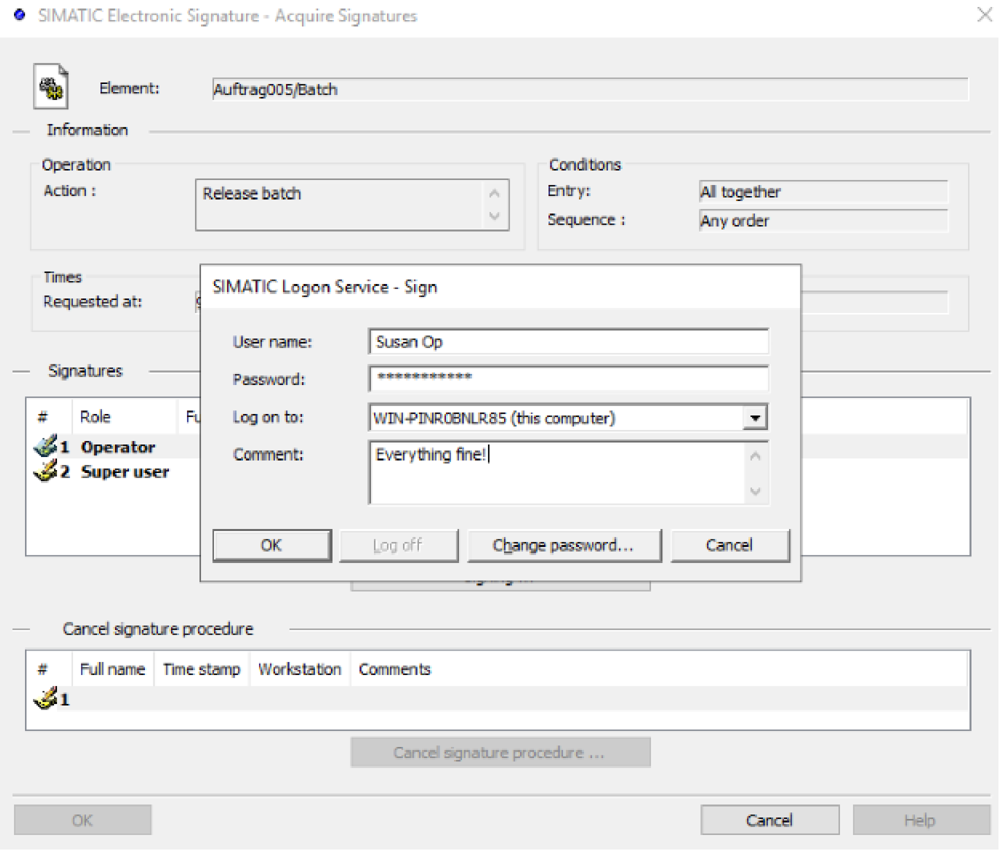


Action	Roles	Sequence
□ Release library for production	0	□
□ Release library for testing	0	□
□ Revoke release of library	0	□
□ Delete library	0	□
☑ Release master recipe for production	1	□
☑ Release master recipe for testing	1	□
☑ Revoke release of master recipe	1	□
□ Delete master recipes	0	□
□ Release formula	0	□
□ Revoke release of formula	0	□
□ Delete formula	0	□

☑ Configure/activate ESIG for batch execution

□ Force comment when signing

A comment can also be entered for each electronic signature; this comment can be forced in the mask shown above.



SIMATIC Electronic Signature - Acquire Signatures

Element: Auftrag005/Batch

Information

Operation
Action : Release batch

Conditions
Entry: All together
Sequence : Any order

Times
Requested at:

Signatures

#	Role
1	**Operator**
2	**Super user**

SIMATIC Logon Service - Sign

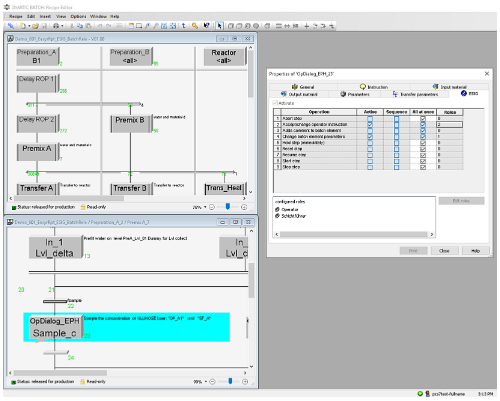
User name: Susan Op
Password: ************
Log on to: WIN-PINR0BNLR85 (this computer)
Comment: Everything fine!

Cancel signature procedure

#	Full name	Time stamp	Workstation	Comments
1				

In addition to these global project rules, object-specific rules can also be created for electronic signatures. The figure below shows some example signature rules for a batch.

The settings are made in the recipe properties.



SIMATIC BATCH: Recipe Editor
Recipe Edit Insert View Options Window Help
Demo_801_EasyRpt_ESIG_BatchRele - V01.00
Preparation_A B1
Preparation_B <all>
Reactor <all>
Delay ROP 1
Delay ROP 2
Premix A
Premix B
Transfer A
Transfer B
Trans_Heat
Status: released for production
Read-only
Demo_801_EasyRpt_ESIG_BatchRele / Preparation_A_2 / Premix A_7
In_1 Lvl_delta
Prefill water on level PreA_Lvl_01 Dummy for Lvl collect
Sample
OpDialog_EPH Sample_c
Sample the concentration of GLUKOSE User: "OP_A1" und "SF_A"
pcs7test-fullname
3:13 PM

Properties of 'OpDialog_EPH_23'

General
Instruction
Input material
Output material
Parameters
Transfer parameters
ESIG

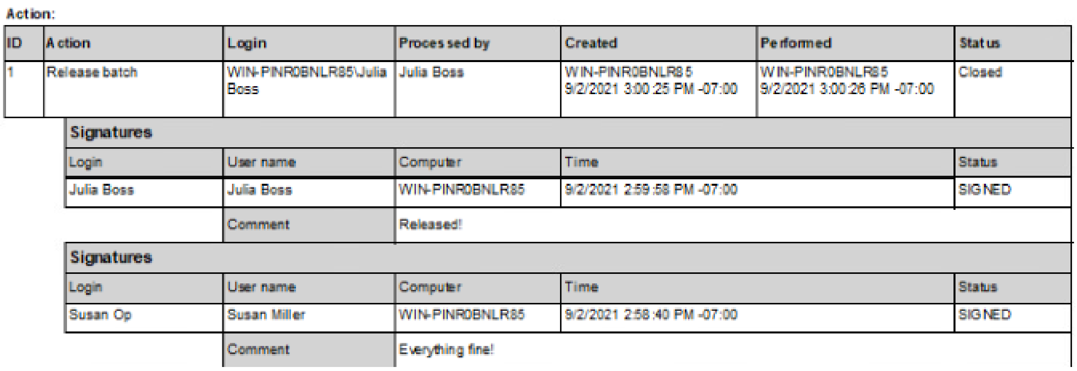
☑ Activate

	Operation	Active	Sequence	All at once	Roles
1	Abort step	□	□	☑	0
2	Accept/change operator instruction	☑	□	☑	2
3	Adds comment to batch element	□	□	☑	0
4	Change batch element parameters	☑	□	☑	1
5	Hold step (immediately)	□	□	☑	0
6	Reset step	□	□	☑	0
7	Resume step	□	□	☑	0
8	Start step	□	□	☑	0
9	Stop step	□	□	☑	0

configured roles
Operator
Schichtführer

Edit roles
Print
Close
Help

The electronic signatures provided are stored in the change log of SIMATIC BATCH and are also available in the report.



Action:

ID	Action	Login	Processed by	Created	Performed	Status
1	Release batch	WIN-PINR0BNLR85\Julia Boss	Julia Boss	WIN-PINR0BNLR85 9/2/2021 3:00:25 PM -07:00	WIN-PINR0BNLR85 9/2/2021 3:00:26 PM -07:00	Closed

Signatures

Login	User name	Computer	Time	Status
Julia Boss	Julia Boss	WIN-PINR0BNLR85	9/2/2021 2:59:58 PM -07:00	SIGNED
	Comment	Released!		

Signatures

Login	User name	Computer	Time	Status
Susan Op	Susan Miller	WIN-PINR0BNLR85	9/2/2021 2:58:40 PM -07:00	SIGNED
	Comment	Everything fine!		

6.10.2 Electronic signatures on PCS 7 OS

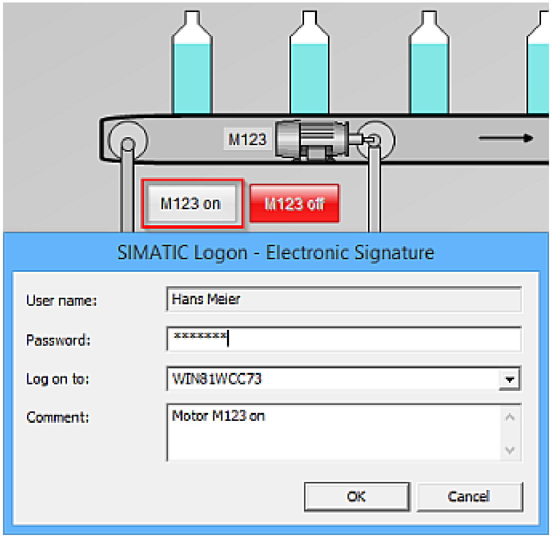
There are various ways to configure an electronic signature for the operating level of PCS 7 OS. These are explained in the WinCC manual, see link below.

See also

- Manual "WinCC: Working with WinCC", chapter 14.10 "Electronic signatures", Online Support under entry ID 109792641 (https://support.industry.siemens.com/cs/ww/en/view/109792641)

Example of a single electronic signature with SIMATIC Logon dialog

SIMATIC Logon offers a dialog to specify an electronic signature. This dialog is opened when the function *Show Dialog* is called in a VB script or C script.



SIMATIC Logon - Electronic Signature

User name: Hans Meier

Password: *******

Log on to: WIN81WCC73

Comment: Motor M123 on

Example of a multiple electronic signature

An application example for configuration of several electronic signatures for one dedicated action on PCS 7 OS is available in the Online Support. However, the compatibility of the example must be verified individually for current system versions.

See also

- Manual "SIMATIC Logon", Online Support under entry ID 109804727 (https://support.industry.siemens.com/cs/ww/en/view/109804727)
- Notes in the "GMP Engineering Manual WinCC", chapter 6.4, Online Support under entry ID 109775436 (https://support.industry.siemens.com/cs/ww/en/view/109775436)
- Application example "Configuring electronic signatures", Online Support under entry ID 66926225 (https://support.industry.siemens.com/cs/ww/en/view/66926225)
- Chapter "OPD – User dialogs and electronic signatures (Page 39)"

6.10.3 Electronic signature on PCS 7 ES

Configuration data in the engineering system are subject to change control, and changes must be documented in a traceable manner. The requirements of 21 CFR Part 11 for audit trails and electronic signatures do not usually apply to engineering systems.

If individual items of data or any inputs or changes made in relation to them have a bearing on quality, they must only be entered via the operator control level (OS) and, if required, assigned an electronic signature at that same location.

6.11 Recording and archiving data electronically

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

The following steps are involved in electronic recording and archiving:

- To determine the data to be archived, the archive sizes and the suitable archiving strategy, see Chapter "Determining the data to be archived (Page 128)"
- Set up process value archives for the online storage of selected process values, see Chapter "Setting up process value archives (Page 128)"
- Archiving batch data, see Chapter "Archiving batch data (Page 130)"
- Long-term archiving, definition of parameters for exporting to the archive server (time period or amount of storage space used), see Chapter "Long-term archiving on a central archive server (Page 131)"

6.11.1 Determining the data to be archived

Various factors, such as those listed below, must be taken into account when defining the archiving strategy and determining the required storage space:

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

In PCS 7, this data is stored in various archives:

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

In other parts of the system further actions are monitored and recorded in log files or databases:

- Change log on ES level for "Downloading the target system" and online parameter changes
- SIMATIC Logon database "EventLog.mdb"
- Event Viewer under Windows Computer Management (logon/logoff activities, account management, permission settings for the file system, etc. according to the corresponding configuration)

Note

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

6.11.2 Setting up process value archives

The procedure for configuring a process value archive is broken down into the following steps:

- Creating the new process value archive and selecting the tags to be stored in the short-term archive.
- Configuring the process value archive by specifying or selecting access permission levels or the storage location, for example.

The process value archive is used to record tag-related process values (analog and binary values) in a database in the form of a short-term archive. The size of the short-term archive is defined in the specifications (URS, FS, DS).

Note

The segments in the short-term archive must be created in such a way that they are exported at regular intervals, ensuring that no data can be lost.

The process values and messages saved in the OS server can be exported to an external drive or transferred to an archive server for long-term archiving.

Accumulated batch data and reports can also be passed on to the archive server by the BATCH server.

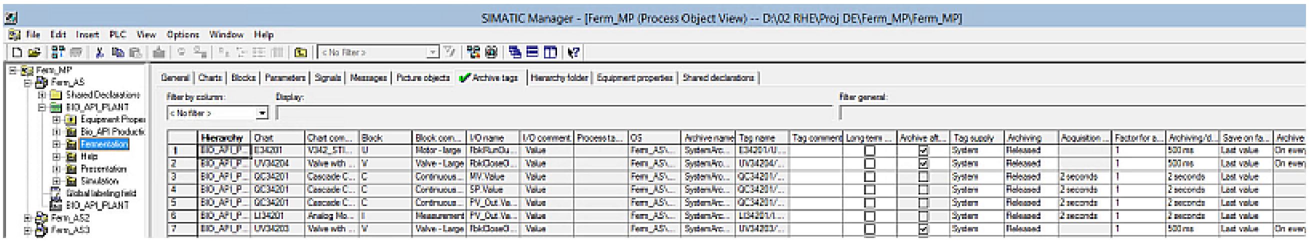
Note

If the connection to the archive server is interrupted, the data is buffered in the short-term archive of the station concerned.

The size of the database is determined by the number of process value archives and the process tags they contain. The size of each process value archive depends on the measurement with the fastest acquisition cycle. Cycle acquisition should be performed uniformly within a process value archive.

It is therefore advisable to always store process tags with the same acquisition cycle (for example, 500 ms, 1 s, 10 s, 1 min) together in one process value archive. As a result, a separate process value archive is configured for each acquisition cycle.

Archiving cycles are specified in the process object view.



	Hierarchy	Chart	Chart com...	Block	Block com...	I/O name	I/O comment	Process ta...	OS	Archive name	Tag name	Tag comment	Long term ...	Archive aft...	Tag supply	Archiving	Acquisition ...	Factor for a...	Archiving/d...	Save on fa...	Archive
1	BIO_API_P...	EI34201	V342_STI...	U	Motor - large	FbkRunOu...	Value		Ferm_AS\...	SystemArc...	EI34201/U...		□	☑	System	Released		1	500 ms	Last value	On every
2	BIO_API_P...	UV34204	Valve with ...	V	Valve - Large	FbkCloseO...	Value		Ferm_AS\...	SystemArc...	UV34204/...		□	☑	System	Released		1	500 ms	Last value	On every
3	BIO_API_P...	QC34201	Cascade C...	C	Continuous ...	MV.Value	Value		Ferm_AS\...	SystemArc...	QC34201/...		□	□	System	Released	2 seconds	1	2 seconds	Last value	
4	BIO_API_P...	QC34201	Cascade C...	C	Continuous ...	SP.Value	Value		Ferm_AS\...	SystemArc...	QC34201/...		□	□	System	Released	2 seconds	1	2 seconds	Last value	
5	BIO_API_P...	QC34201	Cascade C...	C	Continuous ...	PV_Out.Va...	Value		Ferm_AS\...	SystemArc...	QC34201/...		□	□	System	Released	2 seconds	1	2 seconds	Last value	
6	BIO_API_P...	LI34201	Analog Mo...	I	Measurement	PV_Out.Va...	Value		Ferm_AS\...	SystemArc...	LI34201/1...		□	□	System	Released	2 seconds	1	2 seconds	Last value	
7	BIO_API_P...	UV34203	Valve with ...	V	Valve - Large	FbkCloseO...	Value		Ferm_AS\...	SystemArc...	UV34203/...		□	☑	System	Released		1	500 ms	Last value	On every

The specification documents (process tag list, design specification, etc.) contain definitions for the following process value archive parameters, for example:

- Classification of messages which have a bearing on quality and those which do not
- Type of acquisition, cyclic, cyclic-continuous, upon change, etc.
- Cycle time
- Type of value (instantaneous value, average value, maximum value, etc.)

See also

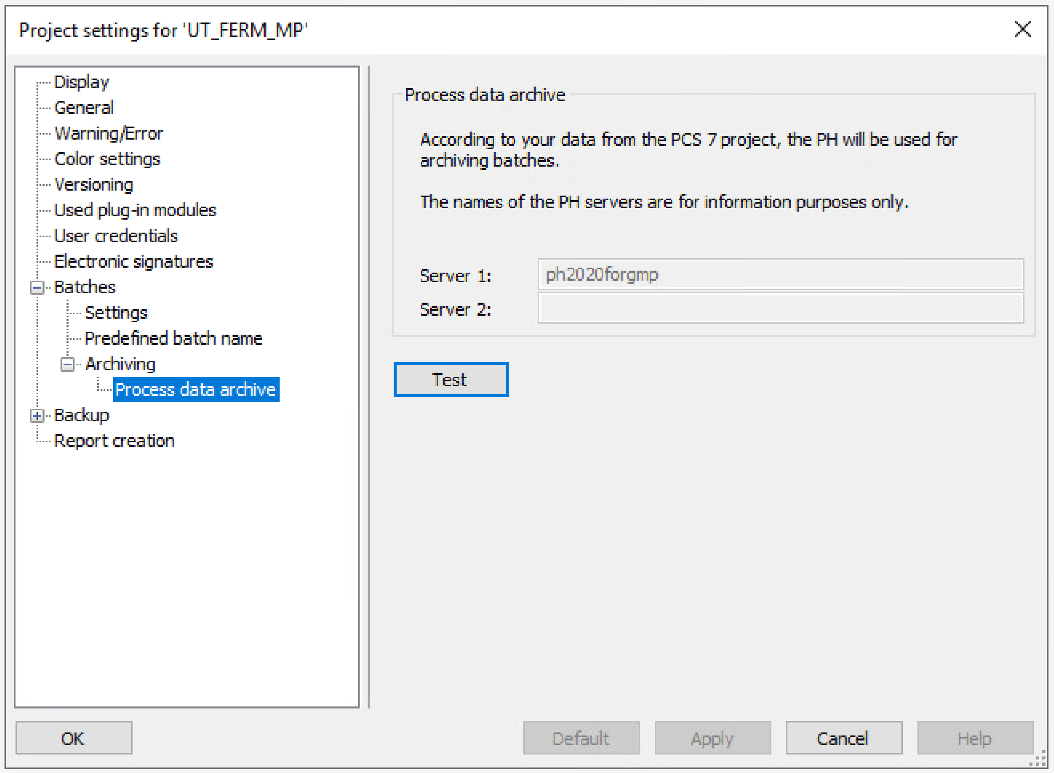
- Manual "WinCC: Working with WinCC", chapter 6 "Archiving process values", Online Support under entry ID 109792641 (https://support.industry.siemens.com/cs/ww/en/view/109792641)
- Manual "PCS 7 Compendium Part A", chapter 10.4.1 "Archiving – Introduction", Online Support under entry ID 109809015 (https://support.industry.siemens.com/cs/ww/en/view/109809015)

6.11.3 Archiving batch data

Batches can be archived in long-term archives in BatchCC. The settings for the selection of the preferred archiving method and printing of batch reports are made in the project settings.

See also

- Manual "SIMATIC BATCH", chapter 15.1.2.11, Online Support under entry ID 109794450 (https://support.industry.siemens.com/cs/ww/en/view/109794450).


Project settings for 'UT_FERM_MP'

Process data archive

According to your data from the PCS 7 project, the PH will be used for archiving batches.

The names of the PH servers are for information purposes only.

Server 1: ph2020forgmp
Server 2:

In the example above, a SIMATIC Process Historian was configured for archiving. If "Directory" is selected as archiving path instead, access to this path must be protected via Windows security mechanisms and must only be granted to authorized persons.

6.11.4 Long-term archiving on a central archive server

A separate server PC is used for long-term archiving, either in form of individual segments or on the SIMATIC Process Historian. This is used for the long-term archiving of messages, process values, and reports.

Process values and messages exported from the OS archives as well as OS reports and batch data of SIMATIC BATCH can be displayed on the system. The system verifies via checksum that the data was not corrupted ("Enable signing").

Segment data remains available in the OS database even after it has been archived. The segment in the OS short-term archive is only deleted when one of the associated parameters "Time period of all segments" or "Max. size of all segments" is exceeded.

See also

- Manual "PCS 7 Operator Station", Online Support under entry ID 109794374 (https://support.industry.siemens.com/cs/ww/en/view/109794374)
- Manual "PCS 7 Compendium Part A", chapter 10.4 "Archiving", Online Support under entry ID 109809015 (https://support.industry.siemens.com/cs/ww/en/view/109809015)
- Link collection "Installation, Operation and Maintenance PH/IS", Online Support under entry ID 66579062 (https://support.industry.siemens.com/cs/ww/en/view/66579062)

Network security

For information on accessing from another network segment (internet/intranet), refer to manual "SIMATIC PCS 7 and WinCC Security Concept".

Integration in Lifebeat Monitoring

The integration of the long-term server is the same as described in chapter "Monitoring PCS 7 Components (Page 111)" for integration of SIMATIC PCS 7 components into Lifebeat Monitoring. An OPC connection simply needs to be set up, via which lifebeat monitoring can be performed.

Audit trail

Changes to archived data are generally not desired. By default, users only have read access to the archived data. The long-term server therefore does not support an audit trail in accordance with 21 CFR Part 11. All events, such as exporting of data to external media or failed exports, are nevertheless saved in a log file directory with the Process Historian.

6.12 Uninterruptible power supply (UPS)

UPS systems are necessary so that process and Audit Trail data, for example, can continue to be recorded during power failures. The design of the UPS must be coordinated with the system operator and specified accordingly. The following items must be taken into consideration here:

- Energy consumption of systems to be supplied
- Performance capability of the UPS
- Desired duration of the UPS battery backup

The energy consumption of the systems with battery backup determines the size of the UPS. A further selection criterion is the priority of the system. Systems with higher priority are:

- Automation system (AS)
- Archiving server
- Operator station (OS) server and clients
- SIMATIC BATCH server and clients
- Network components

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

The use of UPS systems is linked to the installation and configuration of software. The following must be taken into account:

- Configuration of alarms regarding power failure
- Determination of the time frame for shutting down the PC
- Specification of the time frame of the UPS battery backup

The process control system must be programmed so that it is brought to a safe state after a specified buffer time in the event of a power failure.

6.12.1 Configuration of a UPS

The following table contains an example of the configuration of an uninterruptible power supply for an operator station in a process control system. The same basic procedure can be used with automation stations.

Case	Action	Response
1	Power failure <10 seconds	The process control system computers are supplied backup battery power by the UPS. An alarm using a digital input in the process control system documents the power failure.
2	Power failure > 20 minutes. Power returns after 25 minutes	The process control system computers are supplied backup battery power by the UPS. An alarm in the process control system documents the power failure and the shutdown of the process control system after 20 minutes. The UPS stops supplying power after a defined hold time to ensure that the process control system computers can restart independently after restoration of power.
3	Power failure > 1 hour	The process control system computers are supplied backup battery power by the UPS. An alarm in the process control system documents the power failure and the shutdown of the process control system after 20 minutes. The UPS stops supplying power after a defined hold time to ensure that the process control system computers can restart independently after restoration of power.

6.12.2 UPS configuration via digital inputs

In addition to the standard buffering provided by UPS devices, the option of monitoring the power supplies should be used. In this case, the phase is monitored via one or several digital inputs.

The failure of the energy supply can be registered via alarm messages and archived during production in the batch report. This guarantees a complete record of the plant problems.

UPS battery backup of load voltage

The automation CPU is supplied with power by the UPS 24 V module both during voltage dips and longer power failures. The phase monitoring module monitors the status change during a power failure using a digital input that should be designed as a fail-safe input signal. If a power failure occurs, an additional alarm can be generated to inform the operator of the power failure (alarm message). By logging it in the message system, this power failure can be used for subsequent investigations.

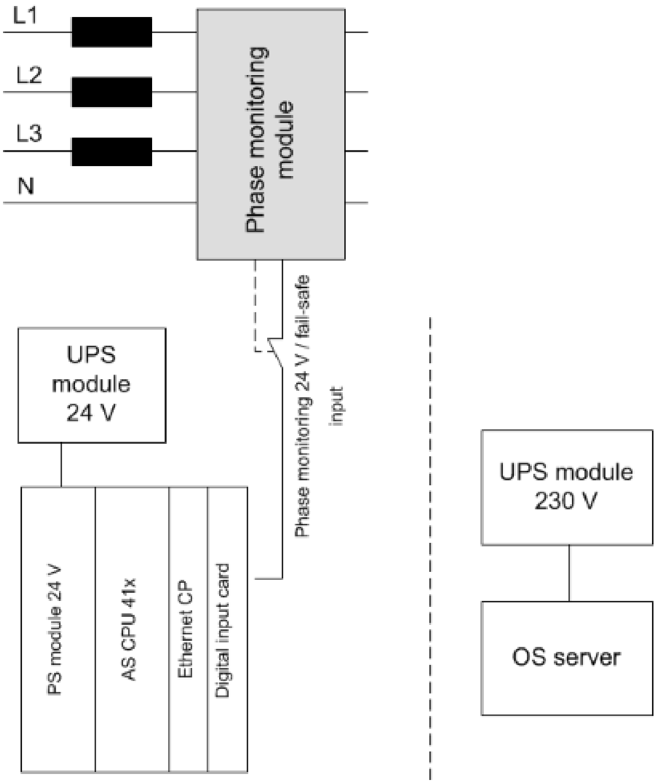
With power failure concepts, safe states can also be implemented immediately or after a certain delay (for example, equipment phase hold, establishing a safe plant status even after power has returned, etc.).

UPS battery backup of power supply

In addition to phase monitoring, the OS server is also buffered, for example by standard UPS 230 V modules. This ensures that the server continues to operate even after a power failure.

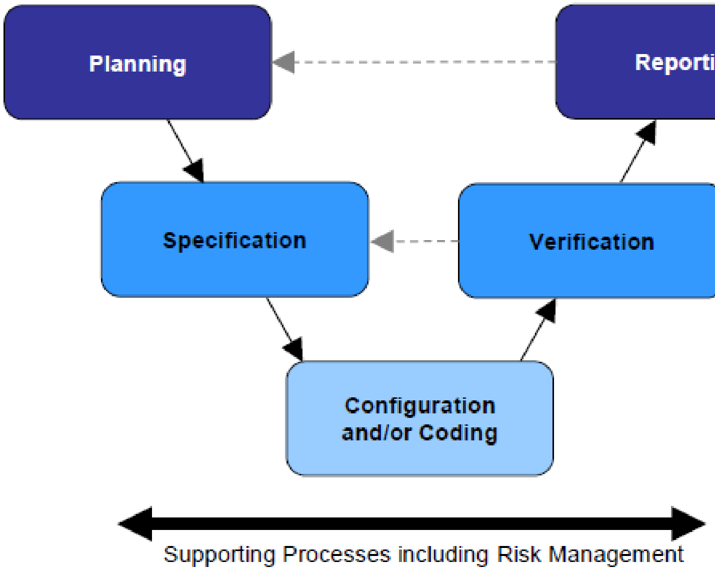
UPS buffering informs the operator of the power failure, by means of alarm messages, for example. Safe states can be introduced by the operator or through automated concepts.

The safe shutdown of the OS server can be indicated by PCS 7 alarm messages and initiated if the power does not return within a specified time. This functionality increases the system availability after power restoration.



Support for Verification 7

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.


Planning
Reporting
Specification
Verification
Configuration and/or Coding
Supporting Processes including Risk Management

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

Various standard functionalities of SIMATIC PCS 7 can be used as support for such verification.

7.1 Test planning

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

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

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

Note

The work involved in testing should reflect not only the results of the risk analysis, but also the complexity of the component to be tested.

A suitable test environment and time, as well as appropriate test documentation, can help to ensure that no or only very few tests need to be repeated during subsequent test phases.

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

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

7.2 Verification of hardware

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

Note

Printouts and screenshots can each be used as evidence. Use of the SIMATIC Management Console proves useful here.

A visual inspection of the hardware can also be performed.

Verification of field devices

Field devices are specified and tested by means of the following information, for example:

- Identification of manufacturer and type
- Order number
- Function/installation location
- Process tag name/measuring range/unit of measure
- Connection type
- Address number

Note

SIMATIC PCS 7 Asset Management can offer support here.

Verification of the automation hardware

Automation stations are specified and tested by means of the following information, for example:

- Identification of manufacturer and type
- Order number
- Number of racks
- Verification of the hardware components used (CPU, CP, etc.)
- Number of distributed I/O stations
- Interfaces to third-party systems
- Address number

Note

HW Config printouts and those with SIMATIC Management Console support the relevant documentation.

The control cabinet documentation must also comply with HW Config.

Verification of the network structure

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

- Name of station, PC, AS, clients, etc.
- Communication module, type of connection and communication partner (Ethernet, PROFIBUS, PROFINET, serial, etc.)
- MAC address (when using the ISO protocol on the plant bus)
- TCP/IP address and subnet mask (when using clients)
- PROFIBUS addresses
- PROFINET device names

Note

The SIMATIC NetPro configuration can be printed out.

Verification of the employed PC hardware

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

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

Note

Utilities can read detailed information about the configuration of the computer and print it as a documented proof. SIMATIC Management Console can be used to perform this from a central point across the entire plant.

7.3 Verification of software

7.3.1 Software categorization according to GAMP 5 Guide

According to the GAMP 5 Guide, the hardware and software components of a system are divided into categories. This assignment can serve as a criterion when determining the suitable lifecycle strategy. The boundaries between categories 3 to 5 should be considered as flowing in this case and not as rigid.

In terms of a PCS 7 system, this means that the individual components require different amount of effort for specification and testing depending on their software category. However, components within each category can have different levels of complexity and/or be more or less critical and must be treated accordingly.

In addition to the literature references cited below, the following tables serve as an instruction and examples. They do not contain a complete list.

Category 1: Infrastructure software **Scope of the testing:** **- Check and document the version number** **- Check and document the correct installation** **- Check in case of configuration**	
Operating system	For example, Microsoft Windows
Server, clients	Physical or virtual, combination of HW Cat. 1 and SW Cat. 1
Database manager	For example, backup system
Programming languages	For example, CFC/SFC editor, recipe editor, graphic editor
DCS development tools	For example, Import/Export Assistant
Configuration management tools	For example, Version Trail, Version Cross Manager
Infrastructure firmware	Can be of different complexity and configurability
Hypervisor	Virtual platform, comparable to operating system
Network monitoring	
Security software	For example, antivirus program, password management

Category 3: Non-configured products or standard functionality **Scope of the testing:** **- Check and document the version number** **- Check and document the correct installation** **- Function test**	
DCS standard functionality	For example, alarm history, SIMATIC Logon
Standard blocks, libraries	For example, APL library including standard faceplates
Parameter settings	Network settings, backup path, access rights
PLC with firmware	For example, S7-300/400
Firmware-based application	Device with standard functionality
Device parameters	For example, I/O range, PID parameters, alarm limits
Smart Transmitter	
Electronic Chart Recorder	

Category 4: Configured products **Scope of the testing:** **- Check and document the version number** **- Check and document the correct installation and configuration** **- Risk-based test for proof of correct operation as part of the business processes**	
Function Block Diagrams (FBD)	CFC (type and instances), FBD (function block diagram), LAD (ladder logic) based on libraries
SFC application	Configuration comparable to interconnections in CFC, but testing depends on complexity and criticality
DCS graphics (mimic displays)	Configuration of existing block icons and faceplates
Recipe processing	
Batch planning	
Route Control Engineering	Configuring and testing routes
OPC Server/Client, Open PCS 7	Configuring the interface and testing the data contained there
Basic scripts	For example, single line ST code for definition of an action for an operating button

Category 5: Customer-specific applications **Scope of the testing:** **- Check and document the version number** **- Planning and releasing the design** **- Check and document the correct installation, the functions and the source code** **- Risk-based test for proof of correct operation as part of the business processes**	
Block creation	STL (statement list), SCL (structured control language)
DCS/SCADA scripts	For example, VB and C++ scripts
Customer-specific applications	For example, spreadsheet calculations (macro), report templates with Microsoft Reporting Services
BATCH API Interface	Applicative interface to SIMATIC BATCH

While a PCS 7 system configured customer-specifically as a whole would usually have to be assigned to category 4 or sometimes even 5, the individual standard components to be installed (without configuration) should be treated in the same way as category 3 or 1.

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

If "free code" is also programmed, this corresponds to category 5.

See also

- GAMP 5 Guide, Appendix M4 "Hardware and software categories"
- GAMP Good Practice Guide "GxP Process Control Systems", Appendix E1
- GAMP Good Practice Guide "IT Infrastructure Control and Compliance", chapter 2.1

Procedure for functions of category 5

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

1. Creation of a functional description for the software
2. Specification of the function blocks used
3. Specification of the inputs and outputs used
4. Specification of the operator control and monitoring capability
5. Creation of software in accordance with specifications and programming guidelines
6. Testing of the structure for compliance with programming guidelines
7. Testing of the function for compliance with the functional description
8. Approval prior to use and/or duplication

7.3.2 Verification of the installed software

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

- Operating system
- SIMATIC PCS 7 software packages (OS Server/Client, Engineering System, etc.)
- SIMATIC options such as SIMATIC BATCH, SIMATIC Route Control, etc.
- Standard libraries
- Third-party software such as Acrobat Reader, Microsoft Office (Word, Excel), etc.

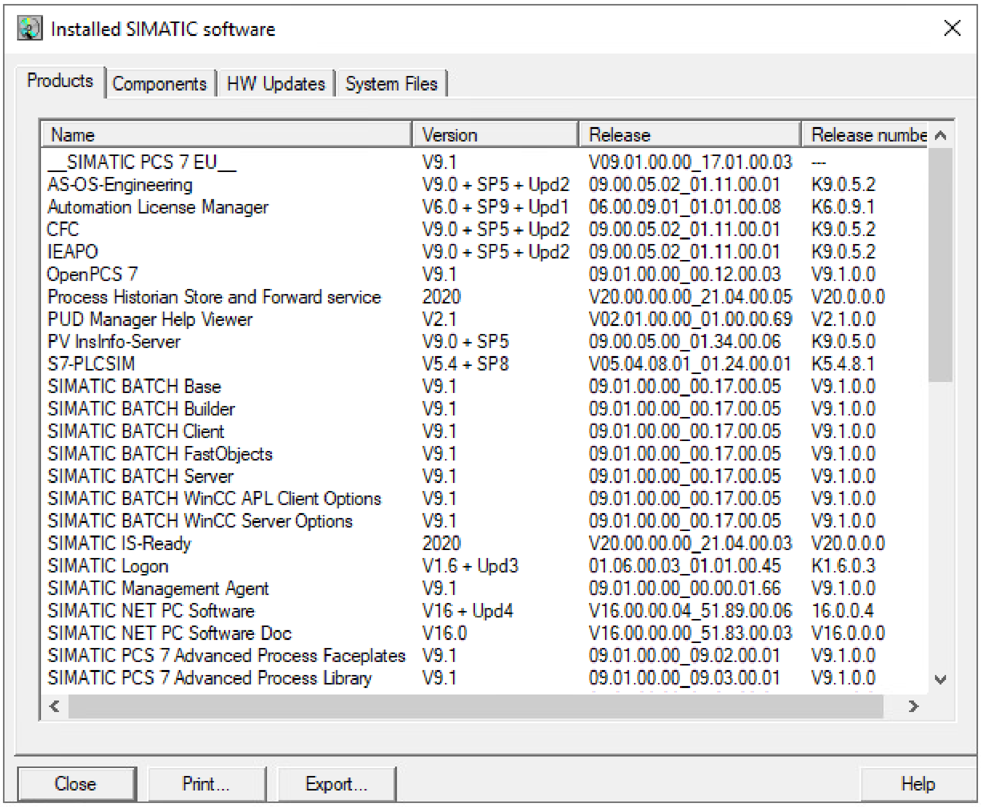
Operating system and other software packages

The installed software can be verified by means of operating system functions. The information can be found in the Control Panel > Add/Remove Programs. All installed software components are displayed there.

Installed SIMATIC software

Installed SIMATIC software can be verified using the "Installed SIMATIC software" software tool. The tool provides information about the SIMATIC software currently installed on the computer; the listing can also be printed or exported.

By using the SIMATIC Management Console, the installed software of all managed computers can be centrally recorded. The work involved in creating such documentation is therefore significantly reduced.



Name	Version	Release	Release numbe
__SIMATIC PCS 7 EU__	V9.1	V09.01.00.00_17.01.00.03	---
AS-OS-Engineering	V9.0 + SP5 + Upd2	09.00.05.02_01.11.00.01	K9.0.5.2
Automation License Manager	V6.0 + SP9 + Upd1	06.00.09.01_01.01.00.08	K6.0.9.1
CFC	V9.0 + SP5 + Upd2	09.00.05.02_01.11.00.01	K9.0.5.2
IEAPO	V9.0 + SP5 + Upd2	09.00.05.02_01.11.00.01	K9.0.5.2
OpenPCS 7	V9.1	09.01.00.00_00.12.00.03	V9.1.0.0
Process Historian Store and Forward service	2020	V20.00.00.00_21.04.00.05	V20.0.0.0
PUD Manager Help Viewer	V2.1	V02.01.00.00_01.00.00.69	V2.1.0.0
PV InsInfo-Server	V9.0 + SP5	09.00.05.00_01.34.00.06	K9.0.5.0
S7-PLCSIM	V5.4 + SP8	V05.04.08.01_01.24.00.01	K5.4.8.1
SIMATIC BATCH Base	V9.1	09.01.00.00_00.17.00.05	V9.1.0.0
SIMATIC BATCH Builder	V9.1	09.01.00.00_00.17.00.05	V9.1.0.0
SIMATIC BATCH Client	V9.1	09.01.00.00_00.17.00.05	V9.1.0.0
SIMATIC BATCH FastObjects	V9.1	09.01.00.00_00.17.00.05	V9.1.0.0
SIMATIC BATCH Server	V9.1	09.01.00.00_00.17.00.05	V9.1.0.0
SIMATIC BATCH WinCC APL Client Options	V9.1	09.01.00.00_00.17.00.05	V9.1.0.0
SIMATIC BATCH WinCC Server Options	V9.1	09.01.00.00_00.17.00.05	V9.1.0.0
SIMATIC IS-Ready	2020	V20.00.00.00_21.04.00.03	V20.0.0.0
SIMATIC Logon	V1.6 + Upd3	01.06.00.03_01.01.00.45	K1.6.0.3
SIMATIC Management Agent	V9.1	09.01.00.00_00.00.01.66	V9.1.0.0
SIMATIC NET PC Software	V16 + Upd4	V16.00.00.04_51.89.00.06	16.0.0.4
SIMATIC NET PC Software Doc	V16.0	V16.00.00.00_51.83.00.03	V16.0.0.0
SIMATIC PCS 7 Advanced Process Faceplates	V9.1	09.01.00.00_09.02.00.01	V9.1.0.0
SIMATIC PCS 7 Advanced Process Library	V9.1	09.01.00.00_09.03.00.01	V9.1.0.0

SIMATIC software licenses

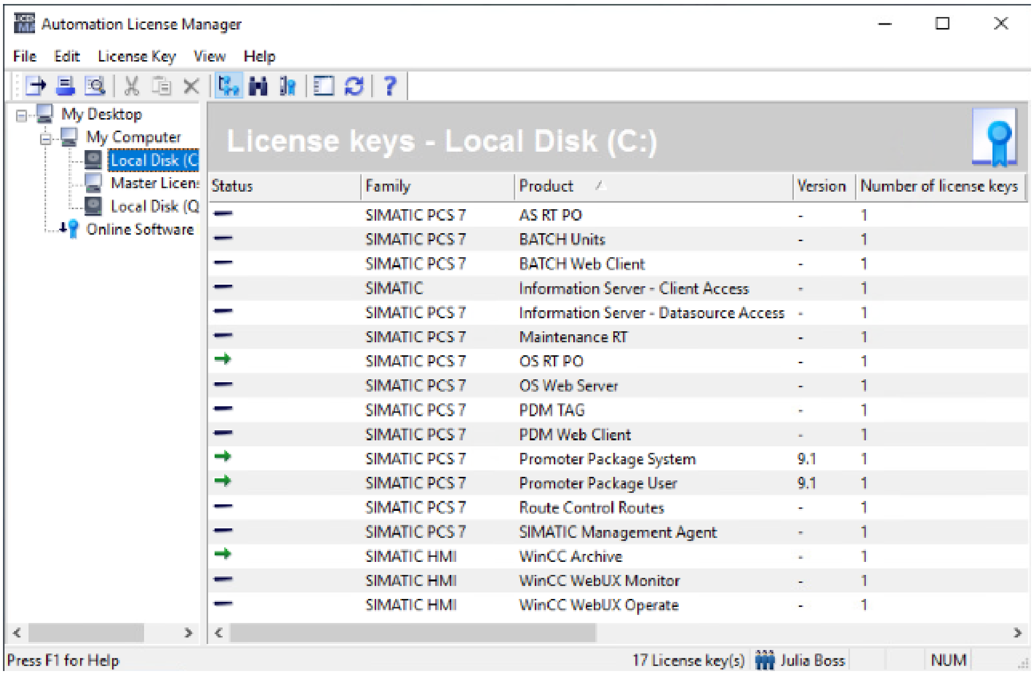
The SIMATIC "Automation License Manager" tool provides information on the licenses currently installed on the PC. For this, the partition of the PC on which the licenses are installed must be selected in the Automation License Manager. The available system licenses are then shown on the right side of the window.

The SMMC also enables central access to the licenses of the managed computers.

The manual "PCS 7 Compendium Part A" contains more information on the documentation of the system installation.

See also

- Manual "PCS 7 Compendium Part A", chapter 4.4.2 "Documentation and inventories", Online Support under
  entry ID 109809015 (https://support.industry.siemens.com/cs/ww/en/view/109809015)

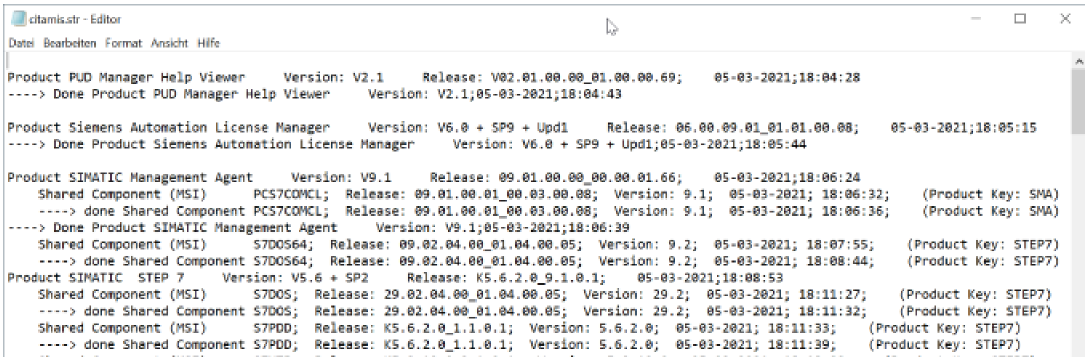


License keys - Local Disk (C:)

Status	Family	Product	Version	Number of license keys
—	SIMATIC PCS 7	AS RT PO	-	1
—	SIMATIC PCS 7	BATCH Units	-	1
—	SIMATIC PCS 7	BATCH Web Client	-	1
—	SIMATIC	Information Server - Client Access	-	1
—	SIMATIC PCS 7	Information Server - Datasource Access	-	1
—	SIMATIC PCS 7	Maintenance RT	-	1
→	SIMATIC PCS 7	OS RT PO	-	1
—	SIMATIC PCS 7	OS Web Server	-	1
—	SIMATIC PCS 7	PDM TAG	-	1
—	SIMATIC PCS 7	PDM Web Client	-	1
→	SIMATIC PCS 7	Promoter Package System	9.1	1
→	SIMATIC PCS 7	Promoter Package User	9.1	1
—	SIMATIC PCS 7	Route Control Routes	-	1
—	SIMATIC PCS 7	SIMATIC Management Agent	-	1
→	SIMATIC HMI	WinCC Archive	-	1
—	SIMATIC HMI	WinCC WebUX Monitor	-	1
—	SIMATIC HMI	WinCC WebUX Operate	-	1

SIMATIC PCS 7 installation log

When SIMATIC PCS 7 is installed, the current status of the installed system programs is saved in the "citamis.str" file. Retro-installations are also documented. The files are in the directory "C:\ProgramData\Siemens\Automation\Logfiles\Setup".



```
Product PUD Manager Help Viewer     Version: V2.1     Release: V02.01.00.00_01.00.00.69;    05-03-2021;18:04:28
----> Done Product PUD Manager Help Viewer     Version: V2.1;05-03-2021;18:04:43

Product Siemens Automation License Manager     Version: V6.0 + SP9 + Upd1     Release: 06.00.09.01_01.01.00.08;    05-03-2021;18:05:15
----> Done Product Siemens Automation License Manager     Version: V6.0 + SP9 + Upd1;05-03-2021;18:05:44

Product SIMATIC Management Agent     Version: V9.1     Release: 09.01.00.00_00.00.01.66;    05-03-2021;18:06:24
    Shared Component (MSI)      PCS7COMCL;  Release: 09.01.00.01_00.03.00.08;  Version: 9.1;  05-03-2021; 18:06:32;    (Product Key: SMA)
    ----> done Shared Component PCS7COMCL;  Release: 09.01.00.01_00.03.00.08;  Version: 9.1;  05-03-2021; 18:06:36;    (Product Key: SMA)
----> Done Product SIMATIC Management Agent     Version: V9.1;05-03-2021;18:06:39
    Shared Component (MSI)      S7DOS64;  Release: 09.02.04.00_01.04.00.05;  Version: 9.2;  05-03-2021; 18:07:55;    (Product Key: STEP7)
    ----> done Shared Component S7DOS64;  Release: 09.02.04.00_01.04.00.05;  Version: 9.2;  05-03-2021; 18:08:44;    (Product Key: STEP7)
Product SIMATIC  STEP 7     Version: V5.6 + SP2     Release: K5.6.2.0_9.1.0.1;    05-03-2021;18:08:53
    Shared Component (MSI)      S7DOS;  Release: 29.02.04.00_01.04.00.05;  Version: 29.2;  05-03-2021; 18:11:27;    (Product Key: STEP7)
    ----> done Shared Component S7DOS;  Release: 29.02.04.00_01.04.00.05;  Version: 29.2;  05-03-2021; 18:11:32;    (Product Key: STEP7)
    Shared Component (MSI)      S7PDD;  Release: K5.6.2.0_1.1.0.1;  Version: 5.6.2.0;  05-03-2021; 18:11:33;    (Product Key: STEP7)
    ----> done Shared Component S7PDD;  Release: K5.6.2.0_1.1.0.1;  Version: 5.6.2.0;  05-03-2021; 18:11:39;    (Product Key: STEP7)
```

7.3.3 Verification of the application software

During verification of the application software, checks are made to verify whether or not the created software meets the requirements of the specifications (FS/DS). You need to consult with the user to agree upon and create the test descriptions (for example for FAT/SAT). These descriptions must take into account the complexity of the software and the design specifications.

The aspects listed below are usually tested, therefore this list can be used as a reference for qualification:

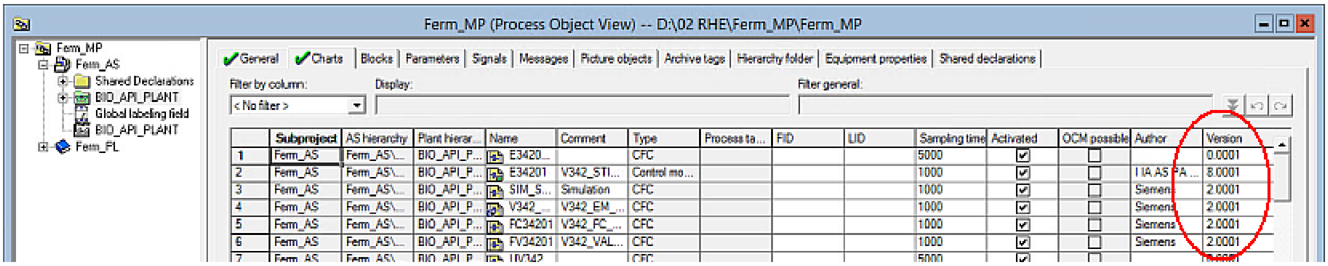
- Check the name of the application software
- Check the plant hierarchy (plant, unit, technical equipment, individual control element, etc.)
- Software module test (typical test)
- Check the communication with other nodes (third-party controllers, MES systems, etc.)
- Check all inputs and outputs
- Check all control modules (individual control level)
- Check all equipment phases and equipment operations (technical functions)
- Check the relationships between operating modes (MANUAL/AUTOMATIC switchovers, interlocks, start, running, stopped, aborting, completed, etc.)
- Check the process tag names
- Check the visualization structure (P&ID representation)
- Check the operator control policies (access control, group permissions, user permissions)
- Check the archiving concepts (short-term archives, long-term archives)
- Check the message concept
- Check the trends, curves
- Check the time synchronization
- Check redundancy switches

Note

If other blocks are needed in addition to the PCS 7 standard libraries in order to configure specific processes or functions, the block libraries (FB, FC, DB) of the PCS 7 Add-on catalog should be used if possible.

If blocks created by the user are to be employed, significantly more work will be required in terms of specification, creation, and verification; this fact should be taken into consideration.

The process object view can be used for testing revisions for verification purposes. The software versions can also be modified there (see figure).



Filter by column: < No filter >

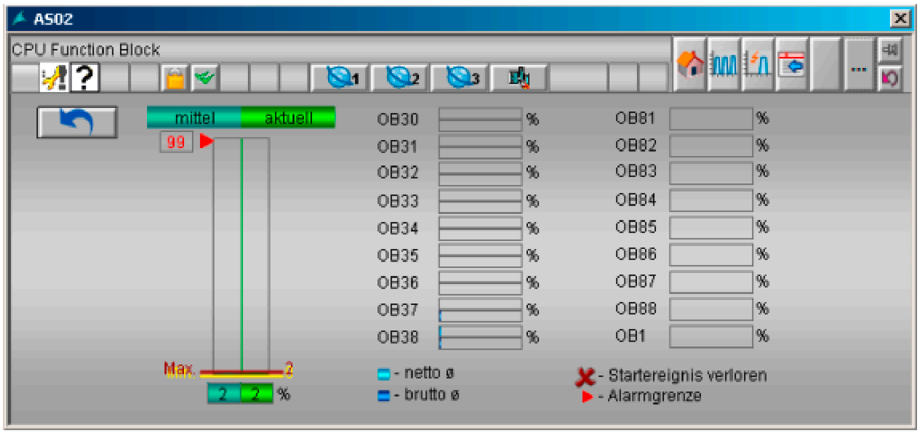
Display:

Filter general:

	Subproject	AS hierarchy	Plant hierar...	Name	Comment	Type	Process ta...	FID	LID	Sampling time	Activated	OCM possible	Author	Version
1	Ferm_AS	Ferm_AS\...	BIO_API_P...	E3420...		CFC				5000	☑	□		0.0001
2	Ferm_AS	Ferm_AS\...	BIO_API_P...	E34201	V342_STI...	Control mo...				1000	☑	□	I IA AS PA ...	8.0001
3	Ferm_AS	Ferm_AS\...	BIO_API_P...	SIM_S...	Simulation	CFC				1000	☑	□	Siemens	2.0001
4	Ferm_AS	Ferm_AS\...	BIO_API_P...	V342_...	V342_EM_...	CFC				1000	☑	□	Siemens	2.0001
5	Ferm_AS	Ferm_AS\...	BIO_API_P...	FC34201	V342_FC_...	CFC				1000	☑	□	Siemens	2.0001
6	Ferm_AS	Ferm_AS\...	BIO_API_P...	FV34201	V342_VAL...	CFC				1000	☑	□	Siemens	2.0001
7	Ferm_AS	Ferm_AS\	BIO_API_P	UV342		CFC				5000	☑	□		[illegible]

Analyzing the CPU load

Asset management can be used to analyze and document CPU utilization.



AS02

CPU Function Block

mittel aktuell

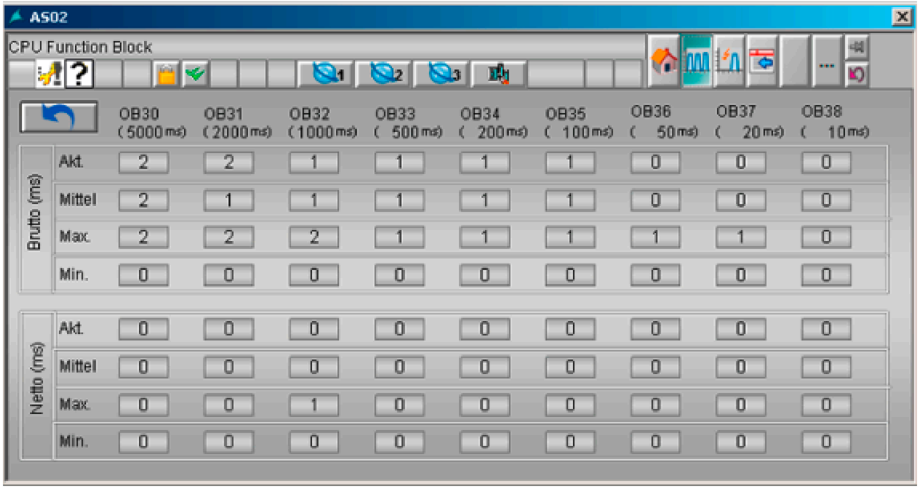
99

Max. 2

2 2 %

OB30	%	OB81	%
OB31	%	OB82	%
OB32	%	OB83	%
OB33	%	OB84	%
OB34	%	OB85	%
OB35	%	OB86	%
OB36	%	OB87	%
OB37	%	OB88	%
OB38	%	OB1	%

🟦 - netto ø
🟦 - brutto ø
✗ - Startereignis verloren
▶ - Alarmgrenze



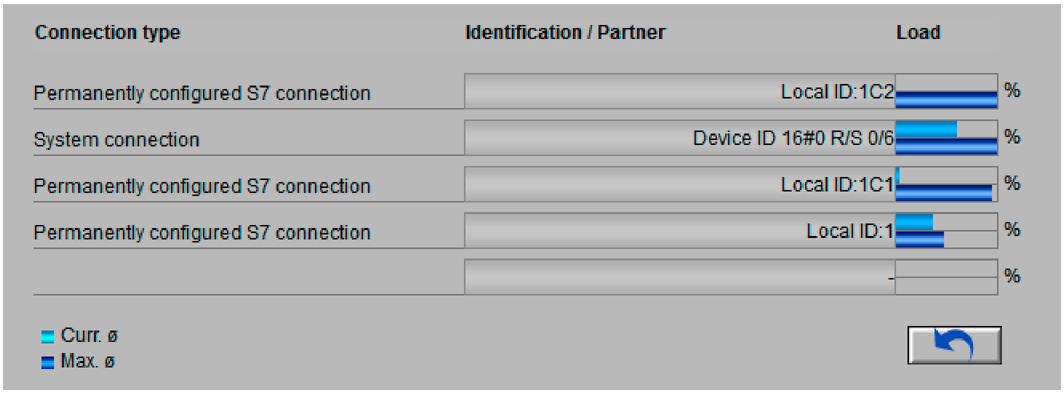
AS02

CPU Function Block

		OB30 (5000ms)	OB31 (2000ms)	OB32 (1000ms)	OB33 (500ms)	OB34 (200ms)	OB35 (100ms)	OB36 (50ms)	OB37 (20ms)	OB38 (10ms)
Brutto (ms)	Akt.	2	2	1	1	1	1	0	0	0
	Mittel	2	1	1	1	1	1	0	0	0
	Max.	2	2	2	1	1	1	1	1	0
	Min.	0	0	0	0	0	0	0	0	0
Netto (ms)	Akt.	0	0	0	0	0	0	0	0	0
	Mittel	0	0	0	0	0	0	0	0	0
	Max.	0	0	1	0	0	0	0	0	0
	Min.	0	0	0	0	0	0	0	0	0

CPU connection utilization

Asset management can also be used to analyze and document CPU connection utilization. This can prove particularly relevant, for example, if certain reserves have been agreed with the customer.



Connection type	Identification / Partner	Load
Permanently configured S7 connection	Local ID:1C2	%
System connection	Device ID 16#0 R/S 0/6	%
Permanently configured S7 connection	Local ID:1C1	%
Permanently configured S7 connection	Local ID:1	%
	-	%

🟦 Curr. ø
🟦 Max. ø

DOCPRO

DOCPRO is a tool for creating and managing plant documentation. SIMATIC PCS 7 V9.1 no longer supports DOCPRO. The compatibility with earlier versions of DOCPRO must be verified for each specific project.

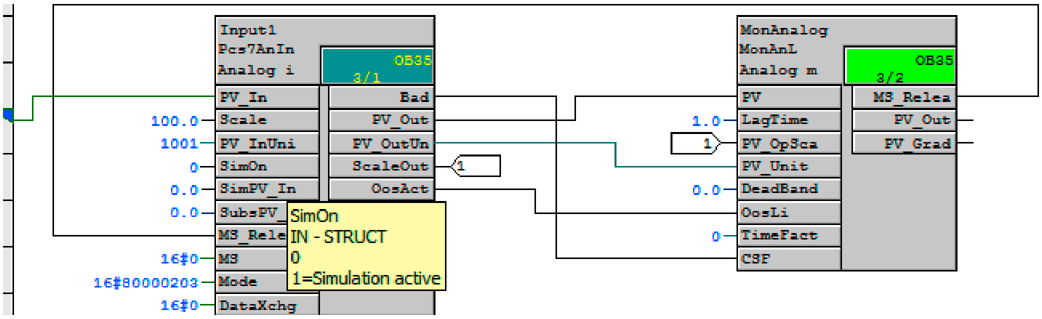
7.3.4 Simulation for test mode

SIMATIC PCS 7 enables the input and output variables of various blocks to be simulated. The simulation is important for test purposes, for example in the context of the FAT, because it allows the project engineer to influence digital and analog inputs and outputs in such a way that complex functions (e.g. temperature control) can be represented and checked.

Enabling simulation

Simulation for test purposes can be enabled at the channel input or channel output driver blocks.

Using the example of a valve, simulation is enabled at the SimOn inputs, and the input can be simulated at the SIMPV_In input.



Disabling simulation

Enabled simulations should be documented in accordance with good practice. After conclusion of the test, all simulations must be deactivated before the plant operation is enabled.

An overview of the APL blocks with active simulation can also be displayed on the OS using the process tag browser.

Note

Where possible, central switches, which are interconnected with all input drivers, can be configured for specific units to enable/disable simulation. On completion of the tests, this central switch can be deleted or disabled, thus switching simulation off from a central location.

Forcing variables

In SIMATIC Manager, one can compile inputs and outputs using a variable table and specify a value using the menu (Variable -> Force). It is also important here to deactivate the forcing again for ALL variables once the test has been performed.

SIMIT simulation software

SIMIT enables a software test to be performed via a simulation platform, without the need for the actual field devices. SIMIT simulates field devices and facilitates versatile use of simple signal tests at the touch of a button, through to complex function tests (such as temperature control).

Used in conjunction with the S7 PLCSIM PLC or SIMIT Virtual Controller (VC) simulation software, which emulates the CPU of an automation system, it enables software tests to be performed without an automation station or field devices and can be used by the software provider to perform the Factory Acceptance Test (FAT), for example.

Use of SIMIT:

- I/O simulation
- Process simulation
- Virtual acceptance tests and commissioning support
- Operator training

Note

SIMIT is ideally suited for use on a test or simulation system. Almost all design-specific and functional errors can be detected early and remedied before the actual commissioning. In production, changes requiring validation can be simulated and tested beforehand, for example.

See also

- Manual "SIMIT", Online Support under entry ID 109801804 (https://support.industry.siemens.com/cs/ww/en/view/109801804)

Simulation hardware Simulation Unit (SU)

In connection with SIMIT software, the Simulation Unit enables a software test without requiring field devices. The SU basically provides a hardware interface for SIMIT.

The SU features PROFIBUS and PROFINET interfaces, which are connected to the AS in a similar way to PROFIBUS or PROFINET and simulate the hardware. The advantage here is that the real hardware interface of the AS is directly addressed, which makes the test more realistic. This increases the probably of discovering errors prior to commissioning and therefore reducing them.

The SU is not a direct successor of the SIMBA Box, but it replaces it technically.

7.4 Configuration control

7.4.1 Versioning of projects with Version Trail

SIMATIC PCS 7 Version Trail can be used to save and archive multiprojects, single projects, and project-specific libraries with a unique version ID. This is performed in accordance with the PCS 7 archiving procedure. Project-specific libraries are also backed up when a multiproject is archived and thus remain associated with the corresponding multiproject.

SIMATIC PCS 7 Version Trail ensures continuous incrementing of the version according to validation factors. A completed version can no longer be changed. However, any archived version can be reloaded in the system using Version Trail or in SIMATIC Manager.

Since GMP requirements demand that SIMATIC Logon be used, all relevant actions are saved with details of the logged-on user.

Note

Before a multiproject is archived, a check must be performed to ensure that no projects or libraries belonging to the multiproject have been removed. This is because only projects and libraries contained in the multiproject at the time of archiving will actually be archived.

The projects to be archived must not be open in the SIMATIC Manager.

In a validated plant, previous project versions can be read back (retrieved) only in exceptional cases and after joint planning with the plant operator.

See also

- Manual "PCS 7 Engineering System", chapter 15.5.3, Online Support under entry ID 109800500 (https://support.industry.siemens.com/cs/ww/en/view/109800500)
- Online help of SIMATIC PCS 7, topic "Version Trail"

Note

The project structure is only adopted once when an archive is created. Subsequent changes in the actual project will not be adopted by Version Trail and must be handled manually.

The representation in Version Trail does not affect the actual archiving. However, automatic archiving operations can only be created from the visible elements.

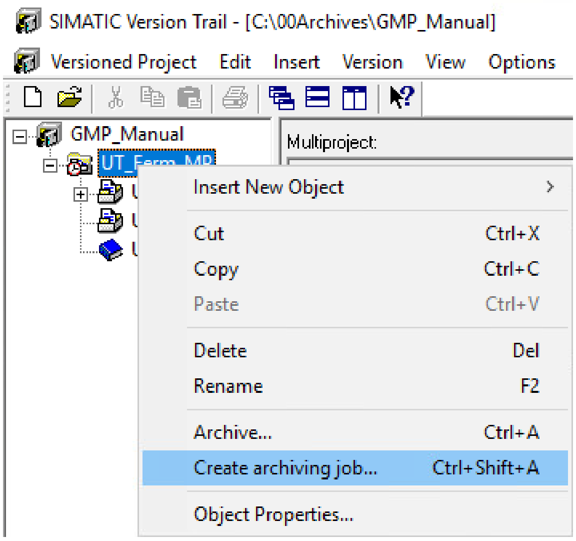
Automatic archiving following download

With the "Archive project after successful download" function, when using SIMATIC Version Trail, once the project has been successfully downloaded, a project backup is made of the downloaded software version.

Automatic archiving - Time-controlled

Version Trail also allows automatic archiving and versioning of multiprojects, projects, and libraries at defined times, including time-controlled readback of block parameters. The Windows Task Manager initiates the execution of the respective jobs.

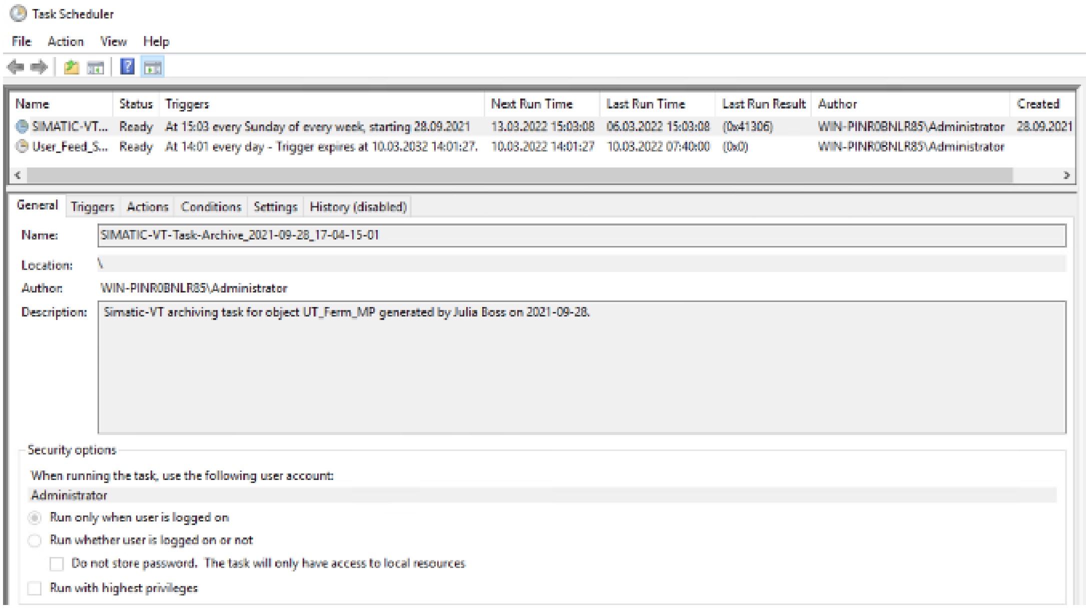
For this it is necessary to select "Create archiving job..." in the shortcut menu of the desired object (multiproject, project, library).



Only one single archiving job can be created for each object! If an archiving job already exists for an object, this procedure can also be used to modify it.

In the displayed dialog window, click the "Create/edit archiving job" button to open the Windows Task Manager. Here, you can modify the parameters and initiate execution of the created jobs.

In Windows Task Manager, double-click the relevant job in the "Simatic VT" folder to select it. This opens its properties.


Task Scheduler
File Action View Help
General Triggers Actions Conditions Settings History (disabled)

Name	Status	Triggers	Next Run Time	Last Run Time	Last Run Result	Author	Created
SIMATIC-VT...	Ready	At 15:03 every Sunday of every week, starting 28.09.2021	13.03.2022 15:03:08	06.03.2022 15:03:08	(0x41306)	WIN-PINR0BNLR85\Administrator	28.09.2021
User_Feed_S...	Ready	At 14:01 every day - Trigger expires at 10.03.2032 14:01:27.	10.03.2022 14:01:27	10.03.2022 07:40:00	(0x0)	WIN-PINR0BNLR85\Administrator	

Name: SIMATIC-VT-Task-Archive_2021-09-28_17-04-15-01

Location: \

Author: WIN-PINR0BNLR85\Administrator

Description: Simatic-VT archiving task for object UT_Ferm_MP generated by Julia Boss on 2021-09-28.

Security options

When running the task, use the following user account:

Administrator

● Run only when user is logged on

○ Run whether user is logged on or not

□ Do not store password. The task will only have access to local resources

□ Run with highest privileges

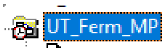
The appropriate settings must be made on the "General" and "Triggers" tabs. In so doing, special attention must be paid to the security options for the user account on the "General" tab. At this point it can be specified whether or not the user has to be logged on for the archiving to run and the privileges with which archiving will be run. The user under which the archiving was run then also appears in the version table in Version Trail.

Note

Descriptive information about the task should be entered in "Description" on the "General" tab. This includes the name of the action, the name of the versioned object to be archived, the name of the person who created the job, and the date the job is created/modified.

The archiving job must now be activated in the "Create archiving job" dialog window. Here, it can also be specified whether the CPUs will be read back before the archiving operation.

The clock symbol next to the archiving job indicates that it is activated.



A notice appears on the screen 20 seconds before an automatic job is run. It can still be canceled during this period.

Note

Version Trail must **not** be open at the time a job is run, since this will prevent the job from running.

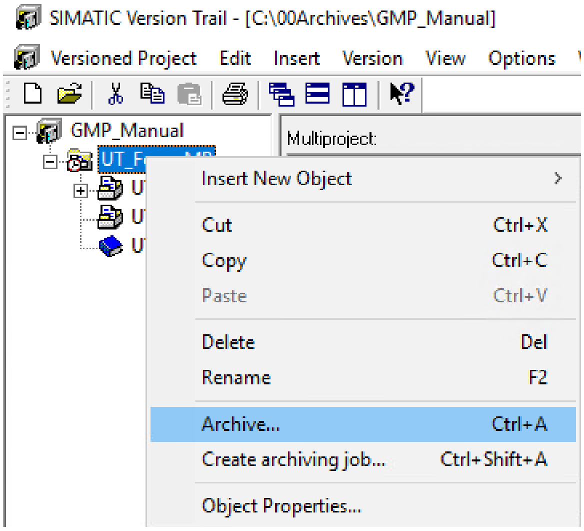
Automatic readback

The Windows Task Manager also initiates the automatic readback of online parameters if a corresponding readback job exists. This job can be created via the shortcut menu of a CPU.

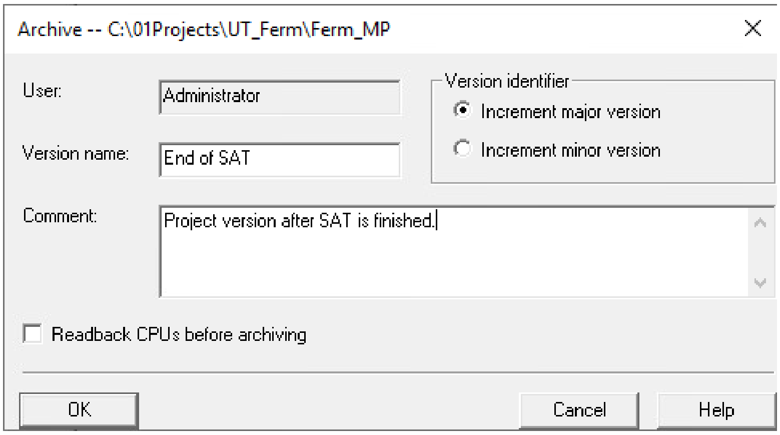
The same procedure is used to create a readback job as for an archiving job. The only difference to an archive job is the selection of the readback scope. Here, it is possible to select between all parameters, parameters that can be controlled and monitored, or marked parameters.

Manual archiving and readback

Version Trail also offers the option to perform manual archiving and/or readback. To do this, "Archive..." or "Readback..." must be selected in the shortcut menu of the desired object.



The respective dialog then opens. When manual archiving is performed, it is also possible to specify whether or not the CPUs are to be read back beforehand. A descriptive comment is helpful.



Archive -- C:\01Projects\UT_Ferm\Ferm_MP

User: Administrator

Version name: End of SAT

Comment: Project version after SAT is finished.

Version identifier
● Increment major version
○ Increment minor version

□ Readback CPUs before archiving

With manual archiving, you can choose between major version and minor version when counting up.

Retrieving

Archived objects (multiprojects, projects, libraries) can be retrieved at any time; see however the note at the start of this chapter "Versioning of projects with Version Trail".

The appropriate entry in the version project window of Version Trail must be selected, and the "Retrieve..." item must be selected in the shortcut menu.

Deleting

The procedure used to retrieve archived objects can also be used to delete them. To do so, the "Delete" command must be selected in the shortcut menu of the selected entry. Only the selected entry is deleted.

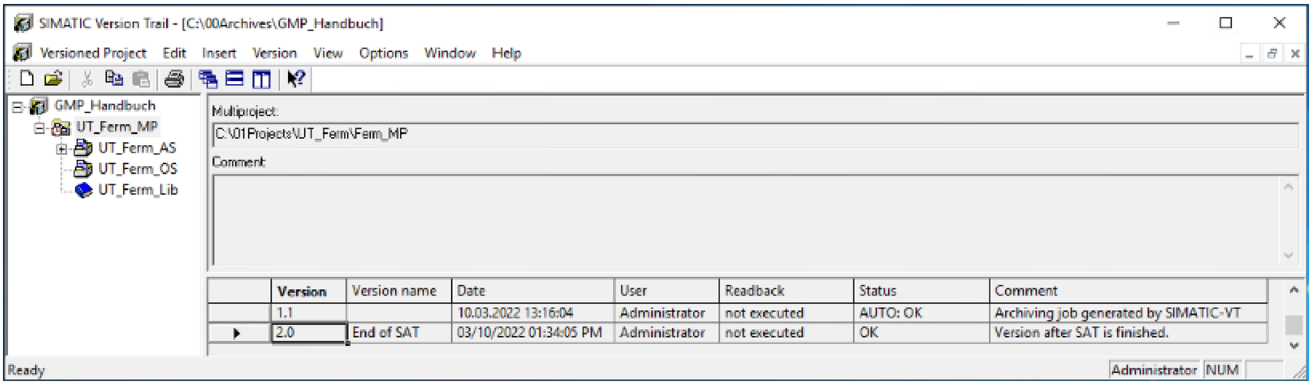
To delete all entries of a versioned archive, the appropriate element must be selected directly in the tree structure and the "Delete" command must be selected in the shortcut menu.

Comparing archived projects

The Version Trail interface enables archived projects to be compared with one another or with online versions. Version Trail makes use of the Version Cross Manager here, by calling it and displaying any differences, see chapter "Version comparison with Version Cross Manager (VXM) (Page 152)" for more information.

Version history

SIMATIC PCS 7 Version Trail manages all actions relating to a versioned project, such as creating, archiving, and deleting versions, in the version history. The version history can be called up using the **Options > Version Trail** menu. All actions relating to the archiving of projects and deletion of versions are logged. The figure below shows the version history, from the creation of versioned project to the archiving of different versions.



SIMATIC Version Trail - [C:\00Archives\GMP_Handbuch]

Multiproject: C:\01Projects\UT_Ferm\Ferm_MP

Comment:

	Version	Version name	Date	User	Readback	Status	Comment
	1.1		10.03.2022 13:16:04	Administrator	not executed	AUTO: OK	Archiving job generated by SIMATIC-VT
▶	2.0	End of SAT	03/10/2022 01:34:05 PM	Administrator	not executed	OK	Version after SAT is finished.

Ready

Administrator NUM

When using SIMATIC PCS 7 Version Trail for continuous archiving, the version history is a good way of documenting different software versions during an automation system’s lifecycle.

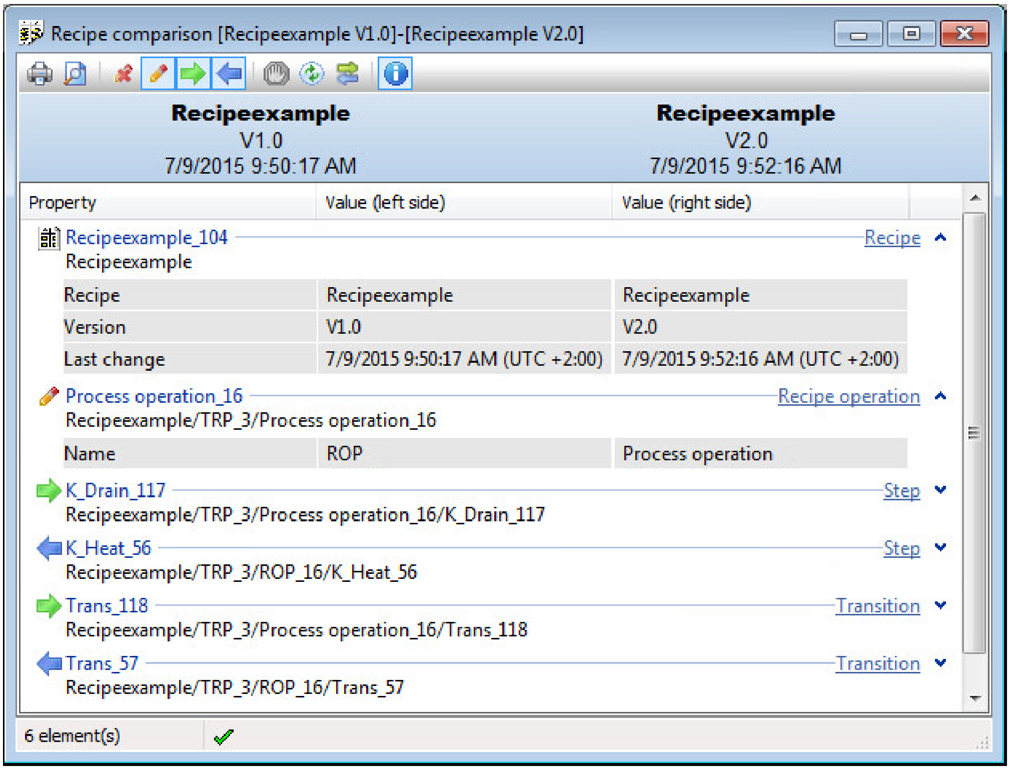
All software versions are listed in chronological order, together with their archiving date and version. This ensures that the latest software version can be copied back in case the application software got lost.

7.4.2 Recipe comparison

Comparison of recipe objects enables a comparison of various versions of master recipes, libraries and formulas.

See also

- Manual "SIMATIC BATCH", chapter 9.5.9, Online Support under entry ID 109794450 (https://support.industry.siemens.com/cs/ww/en/view/109794450).



Recipeexample V1.0 7/9/2015 9:50:17 AM

Recipeexample V2.0 7/9/2015 9:52:16 AM

Property	Value (left side)	Value (right side)
Recipeexample_104 — Recipe Recipeexample		
Recipe	Recipeexample	Recipeexample
Version	V1.0	V2.0
Last change	7/9/2015 9:50:17 AM (UTC +2:00)	7/9/2015 9:52:16 AM (UTC +2:00)
Process operation_16 — Recipe operation Recipeexample/TRP_3/Process operation_16		
Name	ROP	Process operation
K_Drain_117 — Step Recipeexample/TRP_3/Process operation_16/K_Drain_117		
K_Heat_56 — Step Recipeexample/TRP_3/ROP_16/K_Heat_56		
Trans_118 — Transition Recipeexample/TRP_3/Process operation_16/Trans_118		
Trans_57 — Transition Recipeexample/TRP_3/ROP_16/Trans_57		

6 element(s) ✓

7.4.3 Version comparison with Version Cross Manager (VXM)

The Version Cross Manager compares the following objects within projects, for example:

- Library
- Hardware configuration
- CFC/SFC engineering data such as charts, types, chart folders, block folders
- S7 program, S7 blocks, S7 symbols
- Shared declarations
- Messages

The projects to be compared are executed synchronously, i.e. the object trees of the corresponding software structures are compared attribute by attribute. Any differences detected by the comparison are highlighted in color in a results tree.

Saving or printing differences between projects

The differences between projects detected by the comparison can be saved in a .csv file or printed out. The VXMs earlier reporting function can still be used in newer versions of PCS 7, see support entry.

The following information is displayed:

- Additional objects contained in project A
- Additional objects contained in project B
- Differences between project A and project B

For information on operational change control, see chapter "Operational change control (Page 164)".

See also

- FAQ "Using the report function in VXM", Online Support under entry ID 109755393 (https://support.industry.siemens.com/cs/ww/en/view/109755393)

7.4.4 Configuration control with "versiondog"

The PCS 7 Add-on "versiondog" combines the functionalities of SIMATIC Version Trail and Version Cross Manager and its scope of functions goes beyond this. It can be used as a central tool for data backup, change control and software versioning.

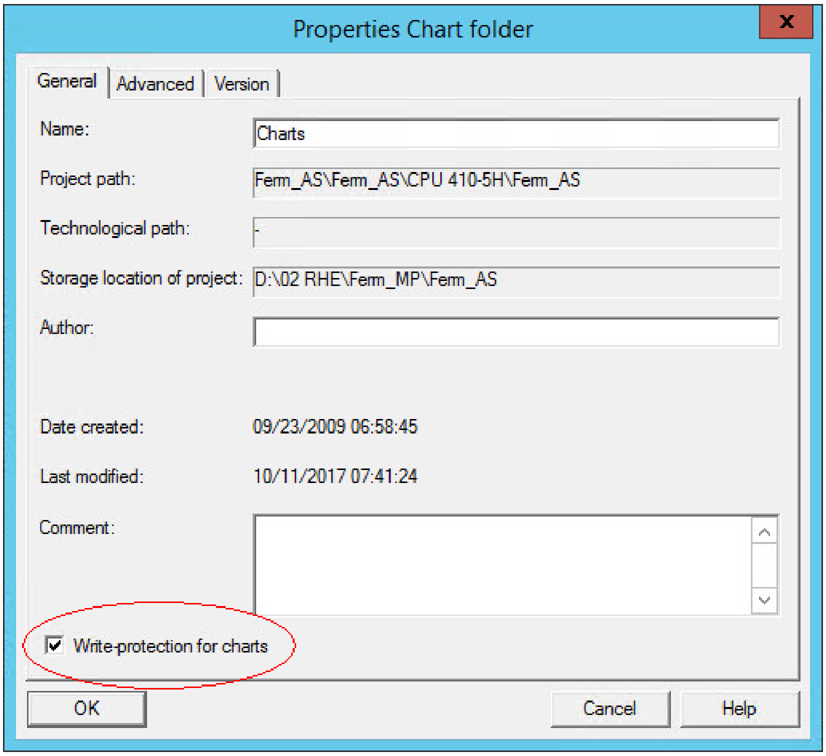
Additional notes can be found in chapter "versiondog – Version assignment and configuration control (Page 38)" and in the PCS 7 Add-on catalog.

7.5 Write protection

7.5.1 Write protection for CFCs/SFCs and SFC types

CFCs/SFCs and SFC types can be provided with write protection to ensure safe operation of the plant after commissioning and verification. If the write protection is enabled, the operating and maintenance personnel can only open CFC/SFCs and SFC types and monitor process values online. They cannot perform intentional or unintentional changes to charts and types.

To enable write protection, "Write-protection for charts" can be selected in the properties of the chart folder for each automation station.



Properties Chart folder

Name: Charts

Project path: Ferm_AS\Ferm_AS\CPU 410-5H\Ferm_AS

Technological path: -

Storage location of project: D:\02 RHE\Ferm_MP\Ferm_AS

Author:

Date created: 09/23/2009 06:58:45

Last modified: 10/11/2017 07:41:24

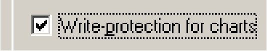
Comment:

☑ Write-protection for charts

The project staff also has the option of enabling or disabling write protection for individual charts or SFC types.

The check box for "Write-protection for charts" can be shown here in two different ways.

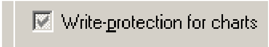
Write protection is selected for all charts in the figure below



☑ Write-protection for charts

White background with black check mark:

Only some charts or SFC types are write-protected in the figure below.

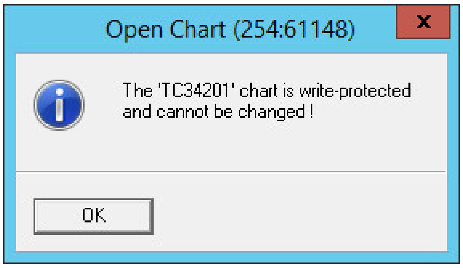


☑ Write-protection for charts

Shaded background and gray check mark:

If the write protection is not enabled for all charts, disabling and enabling write protection for the "Charts" folder once enables write protection for all CFC/SFCs and SFC types of each automation station.

If the chart of a CFC/SFC or SFC type is open, you will see the following notice with write-protected charts:



Open Chart (254:61148)

The 'TC34201' chart is write-protected and cannot be changed !

Note

In the process object view, changes can then be made even when the chart folders are read-only.

See also

- Manual "PCS 7 Engineering System", chapter 4.3.4, Online Support under entry ID 109800500 (https://support.industry.siemens.com/cs/ww/en/view/109800500)

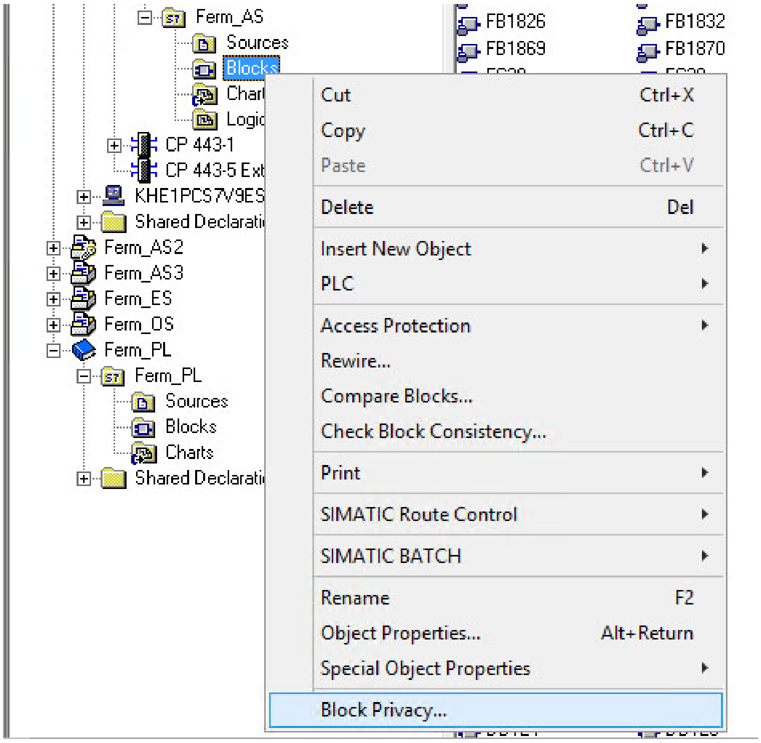
7.5.2 Block encryption with "S7 Block Privacy"

The "S7 Block Privacy" package can be used to encrypt and decrypt function blocks (FB) and functions (FC). It is not possible to encrypt other blocks, such as organization blocks (OB), fail-safe blocks, or blocks with "Know-how protection". The encryption occurs directly in the database of a project. All FBs and FCs that have been encrypted and downloaded to the AS have the status "S7 Block Privacy".

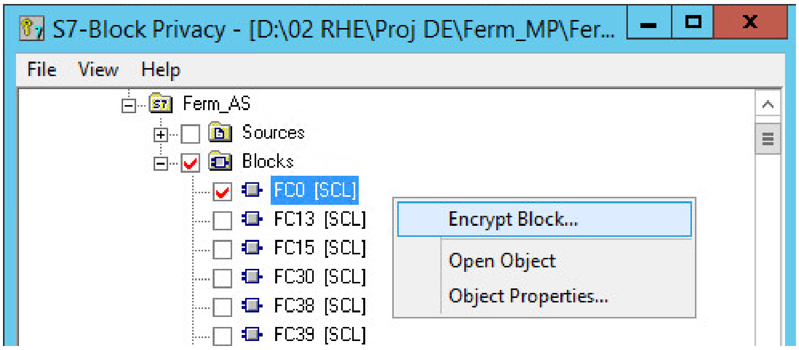
"S7 Block Privacy" provides greater security than the previous Know-How protection and should therefore be used preferentially for sensitive areas in particular.

Procedure

To encrypt blocks, the "Block Privacy" command must be selected in the shortcut menu of a block folder.



The tree structure of the encryption tool lists all blocks and SCL sources in the project. The selection marked with a check mark can be encrypted using the "Encrypt Block..." command in the shortcut menu. This opens a dialog whose instructions must be followed.



SCL sources

SCL sources that are contained in the project and whose blocks have been encrypted should be deleted before transferring the project to third parties. This action can also be performed in the "S7 Block Privacy" application. The "Delete source" function must be selected in the shortcut menu of the source.

Note

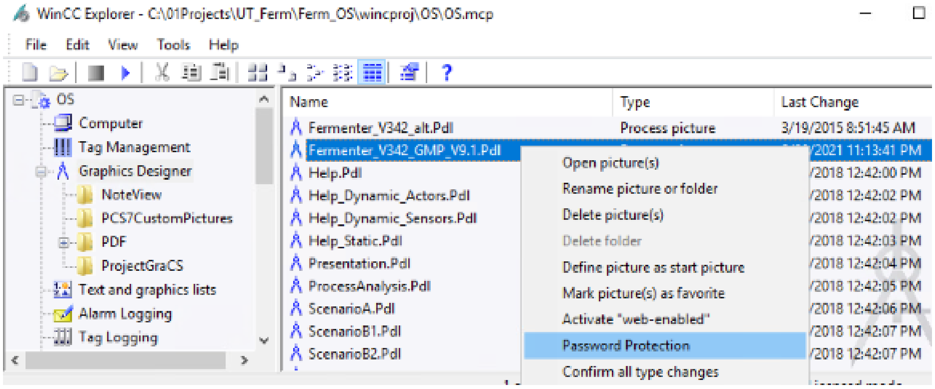
Once the sources have been deleted and are removed from the tree structure, the source folder still has to be reorganized. It is the reorganization step that actually deletes the sources. Before that, the sources are merely designated for deletion and removed from SIMATIC Manager. However, they are still present at the memory location of the project.

Decrypting

The procedure used to encrypt blocks is also used to decrypt them. However, decryption of blocks requires the correct key and the decompilation information.

7.5.3 Protection of graphics

Operating screens can also be protected from modification with a password. The selection is made in the WinCC Explorer by marking one or more screens in the shortcut menu.



7.6 Information on system handover

The following aspects should be clarified at an early stage for the system handover:

- Which documents are transferred in which format.
- Training of operating and maintenance personnel
- Information for system operation, e.g. archiving, backup, calibration
- Reset of simulation, etc.

Note

When the system is handed over, all test accounts must be deleted and standard passwords must be changed!

Data Backup 8

Periodic data backups are not only necessary to avoid data loss during the configuring phase.

They are also necessary during the operation phase to ensure a smooth system restoration in the event of data loss or system failure. An emergency plan is also required for this case.

In addition to the backup of the system installation, the configuration data should also be backed up on a regular basis in order to be able to revert back to the last saved system configuration in the event of a hardware defect or data loss.

The following data backups should be considered:

- Backup of system installation, see chapter "Backup of the system installation (Page 159)"
- Backup of the installation, including all project files (image)
  following system updates and major project changes
  as well as periodically, e.g. every 12 months
- Change-driven backup of project data before/after every change
- Periodic backup or "recopying" of all archived data every 3 to 5 years, for example, to ensure the readability of the data.

Note

The backup of the user software and the backup of the system partition with and without SIMATIC PCS 7 should be stored on external media (for example, CD, DVD, network backup).

See also

- Chapter "System restoration (Page 167)"

8.1 Backup of the system installation

Hard disk images should be used to back up the operating system and the PCS 7 installation. These images allow you to restore the original state of PCs.

Which images are advisable?

- Creation of an image of the operating system installation with all drivers and all settings for the network, user administration, etc., without SIMATIC PCS 7
- Creation of an image of the installed PCs with SIMATIC PCS 7
- Creation of an image of the installed PCs with SIMATIC PCS 7, including all projects

Note

An image can only be imported on a PC with identical hardware. For this reason, the hardware configuration of the PC must be suitably documented, for example using SIMATIC Management Console.

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

8.2 Data backup of the application software

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

See also

- Manual "PCS 7 Service Support and Diagnostics", chapter 3.2 "Data backup", Online Support under entry ID 109794378 (https://support.industry.siemens.com/cs/ww/en/view/109794378)

Backing up user software in the engineering system

The SIMATIC Manager "Archive Project" system function should be used for this purpose or the "Version Trail" option package for version-based archiving.

As of V9.1 SP1, the archived projects can be secured with a hash so that any manipulation of the project is detected.

With the SIMATIC Version Trail option, the project can be backed up manually or in a time-controlled manner and at the same time the versions can be checked. An older version can also be copied via the interface.

See also

- Chapter "Versioning of projects with Version Trail (Page 147)"

Note

If data backups are to be created during plant operation, consideration must be given to whether and, if so, which online parameters must be read back prior to generating the backup.

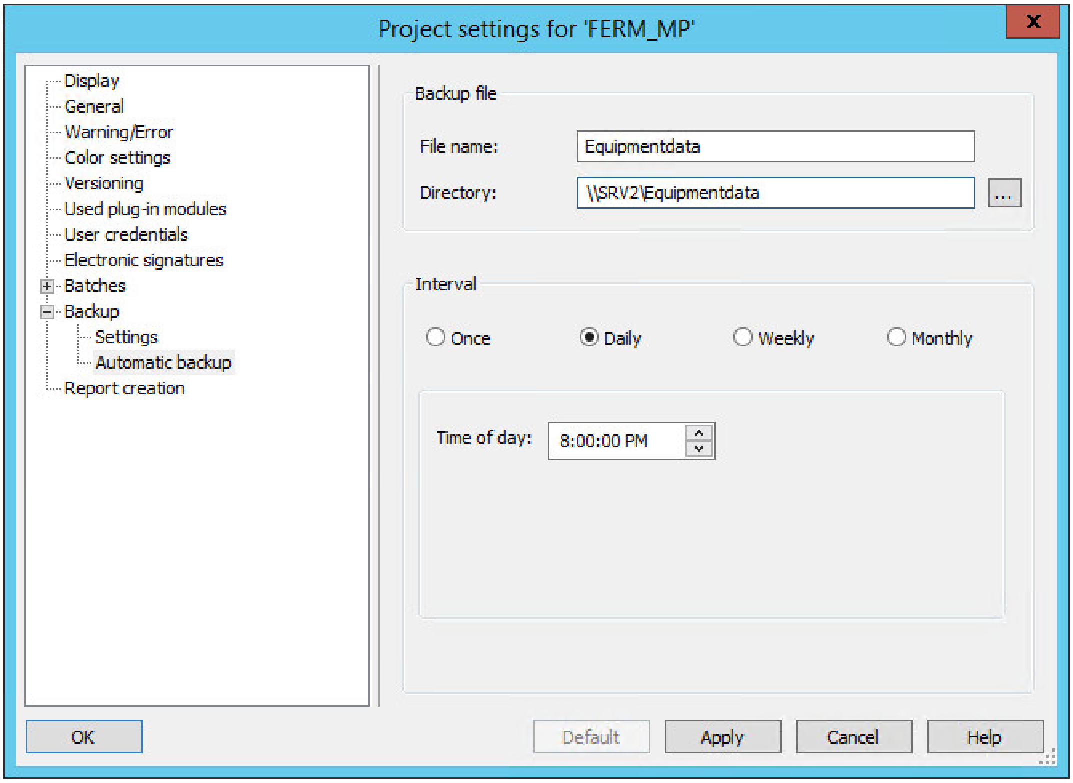
Parameter changes which are not read back will be lost if the system or project is restored.

Backing up recipe data in SIMATIC BATCH

The project configuration must be backed up in PCS 7, as must application data in SIMATIC BATCH (libraries, master recipes, materials, user rights, etc.). This backup is created from within the SIMATIC BATCH Control Center.

SIMATIC BATCH supports automatic and time-controlled backup of BATCH project data. This includes, for example:

- Plant settings
- Project settings
- Libraries
- Formulas
- Master recipes
- Materials



Backup file

File name: Equipmentdata

Directory: \\SRV2\Equipmentdata

Interval

○ Once ● Daily ○ Weekly ○ Monthly

Time of day: 8:00:00 PM

The backup data can be copied back again using the "Restore" command.

Backup of the SIMATIC Route Control configuration

When loading the configuration in SIMATIC Route Control, the Route Control engineering data described for the CSV interface and the material configuration data are automatically exported as of SIMATIC PCS 7 V9.1 SP1.

Operation, Maintenance and Servicing 9

9.1 Operation and monitoring

9.1.1 Process visualization

SIMATIC PCS 7 provides extensive process visualization. Individually configured user interfaces can be created for each application – for reliable process control and optimization of the entire production sequence.

Runtime data can be output by the system based on reports.

9.1.2 User documentation

As of SIMATIC PCS 7 V9.0, the PUD (Plant and User Documentation) Manager Help Viewer is available for offline display of the documentation. It is part of the SIMATIC PCS 7 software package. You can individually extend and update the scope of your user documentation by adding documentation packages.

With the installation of SIMATIC PCS 7, the PUD Manager Help Viewer includes the following documentation:

- SIMATIC PCS 7 Help Center
- OS Process Control

See also

- PUD Manager Explanation and Download, Online Support under entry ID 109748882 (https://support.industry.siemens.com/cs/ww/en/view/109748882)

9.1.3 Audit trail review

In the regulated environment, not only must an audit trail be kept for changes to GMP-critical data, this audit trail must also be audited regularly. This can be accomplished for one thing through regular checking of the functionality while simultaneously incorporating the relevant audit trails in corresponding production reports. For another, evaluations of critical alarms, operator inputs and frequency analyses of messages serve the goal of improving the process.

The following resources can aid the audit trail review:

- Possible contents of an audit trails, see chapter "Audit trail and change control (Page 113)"
- Message classes and priorities, see chapter "Alarm management (Page 106)"

- Options for reporting, see chapters "Reporting (Page 35)" and "Creating reports in SIMATIC BATCH (Page 104)"
- Comprehensive analysis of messages from different sources using the WinCC add-on PM-ANALYZE (https://www.siemens.de/industrysolutions/de/en/wincc/products/pm-analyze/Pages/Default.aspx)

9.2 Operational change control

Any changes to validated plants must always be planned in consultation with the plant operator, documented, and only executed and tested once they have been released.

The following chapters use examples to describe how to make changes:

1. Initiation, description and approval of planned change by plant user
2. Check and backup of the current application software version (project data)
3. Adjustment of system specification
4. Performing the change, including documentation of the performed change (poss. support using tool comparison)
5. Testing the change, including test documentation in suitable form
6. Backup of the changed project with new version ID

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

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

Moreover, in the case of software updates, it might be necessary to make a choice between system security and conformity with the regulations, see also "Updating the system software (Page 170)".

See also

- GAMP 5 Guide, Appendix O6
- GAMP Good Practice Guide "Operation of GxP Computerized Systems", chapter 10

9.3 Servicing and maintenance

Access and authorizations for maintenance personnel must be checked and documented. They must be taken into account in the authorization concept along with the operational rights and the rights for administrators.

Maintenance activities are also changes to the validated complete system. There are often standardized procedures on the operator side for recurring activities, so that a change request is not necessary for each individual action. However, the activities must be scheduled in coordinated fashion and documented in all cases in accordance with the regulations.

9.3.1 Special features of remote maintenance

Various technical options are available for remote access. Depending on the program, to dial in to an external PC station, not only must the user have the appropriate access permission (user name and password), but the Allow remote access authorization must also be enabled. This should however be planned and documented within the scope of the entire system, as access must be controlled. For more on this, see also chapter 3.2 (Page 28) and chapter 4.6 (Page 53).

Note

Setup of remote maintenance functionality must be coordinated with the plant operator. Those responsible for the plant must give their express consent for each individual connection that is established to the system (logon). Changes made by remote access must also be documented in accordance with the operator's instructions.

See also

- Readme PCS 7 V9.1, chapter 3.4.14; Online Support under entry ID 109780270 (https://support.industry.siemens.com/cs/ww/en/view/109780270)

A practical solution could be to assign the logical access permission, but to only establish a physical connection when necessary, and then only when on-site maintenance staff are present.

9.3.2 Asset Management

In the context of process engineering, asset management aims to use appropriate methods to ensure that a production plant benefits from maximum availability at the lowest possible operating costs. The most efficient strategy is without doubt status-oriented maintenance, which must be based on a status detection procedure that is as continuous as possible. Asset management relies on having access to precise information relating to the current plant status, which can then be used to determine exactly which maintenance activities need to be carried where and at what time.

Implementation in PCS 7

The asset management integrated in SIMATIC PCS 7 is used for plant maintenance. Additional hardware and software tools are not required. Plant operators and maintenance engineers use the same SIMATIC PCS 7 tools and user interfaces, along with information which has been filtered and prepared according to the field of activity concerned. While the plant operators operate and monitor the process on the PCS 7 operator station (OS), the maintenance engineer uses the maintenance station (MS) to control the hardware structure of the production facility in order to handle the diagnostics and maintenance requirements.

The various components of a PCS 7 plant can be monitored with the diagnostic and maintenance functions integrated in SIMATIC PCS 7.

PCS 7 Maintenance Station (MS) is available in Basic, Standard and PDM versions.

Note

In conjunction with PDM, the advanced diagnostics of the field devices can be opened from any MS client. The device parameters can be read out and processed via a maintenance client.

For documentation about this, see

- Manual "PCS 7 Maintenance Station", Online Support under entry ID 109794384 (https://support.industry.siemens.com/cs/ww/en/view/109794384)
- Manual "PCS 7 Service Support and Diagnostics", Online Support under entry ID 109794378 (https://support.industry.siemens.com/cs/ww/en/view/109794378)
- Manual "PCS 7 Help on PDM", Online Support under entry ID 109794428 (https://support.industry.siemens.com/cs/ww/en/view/109794428)

The maintenance engineer has access to all details of the components and devices when needed, beginning with an overview display (plant view). The overview display uses the standardized symbols to visualize the condition of a component itself and also provides collective information on the conditions of all devices in the lower-level hierarchies.

There are four areas on the top level:

- IPC area (IPCs, server, clients, ES, PH)
- Network area (network switches)
- AS area, which is divided into two subareas
  - CPU area
  - Field device area
- User range (monitoring of system parts based on configured variables such as operating hours or switching cycles)

The group status message shows the OK condition or the seriousness of the problem according to NE107 in traffic light colors.

Maintenance work can be requested directly via the diagnostic faceplate of a monitored component. The request must then be approved by the plant operator (OS) via the standard faceplate before the maintenance engineer can begin the requested service.

Furthermore, the status of the work can be specified and monitored. This is recorded in the form of an operating message and indicated by the symbols. A work instruction number and a comment can be entered for each work request. Service appointments or intervals can also be determined. Once the set interval expires, a system message is automatically created, which indicates the service required, such as calibration necessary.

A report can be created and printed out for each component. The creation of logs for entire device groups can be useful. In this case, it is possible to filter devices by their priority. The requirement here is the corresponding identification of devices, which is performed in SIMATIC Manager. Currently it is possible to identify devices as "important" or "SIF" (safety relevant).

Condition monitoring

It is often necessary to take into account certain process engineering, chemical, and mechanical conditions in a plant's maintenance concept. Condition monitoring (e.g. pump operating points, motor bearing monitoring) is generally used in a preventive capacity in this regard, as the user receives an automatic notification before critical conditions are reached.

PCS 7 Asset Management enables user-specific, maintenance-relevant process variables or parameters to be integrated into the existing diagnostic structure. PCS 7 provides the appropriate interfaces for this: a function block on the AS and a faceplate on the OS.

9.4 System restoration

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

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

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

There must be a Disaster Recovery Plan which must be checked on a regular basis.

Restoring the operating system and installed software

The operating system and installed software are restored by loading the corresponding images (see chapter "Data Backup (Page 159)"). The instructions provided by the relevant software supplier for the data backup application should be followed.

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

Restoring the application software

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

The following steps may be relevant:

- Reading back the data using the software Version Trail
  Version Trail lists all backup states with major and minor version. The selected backup level is read back via the Retrieve button.
- Reading back the data from a manually created backup
- Retrieving recipes
- Retrieving archives
  This concerns the following, depending on the system configuration and the scope of the problem: process data, messages, batch data, log files, etc.

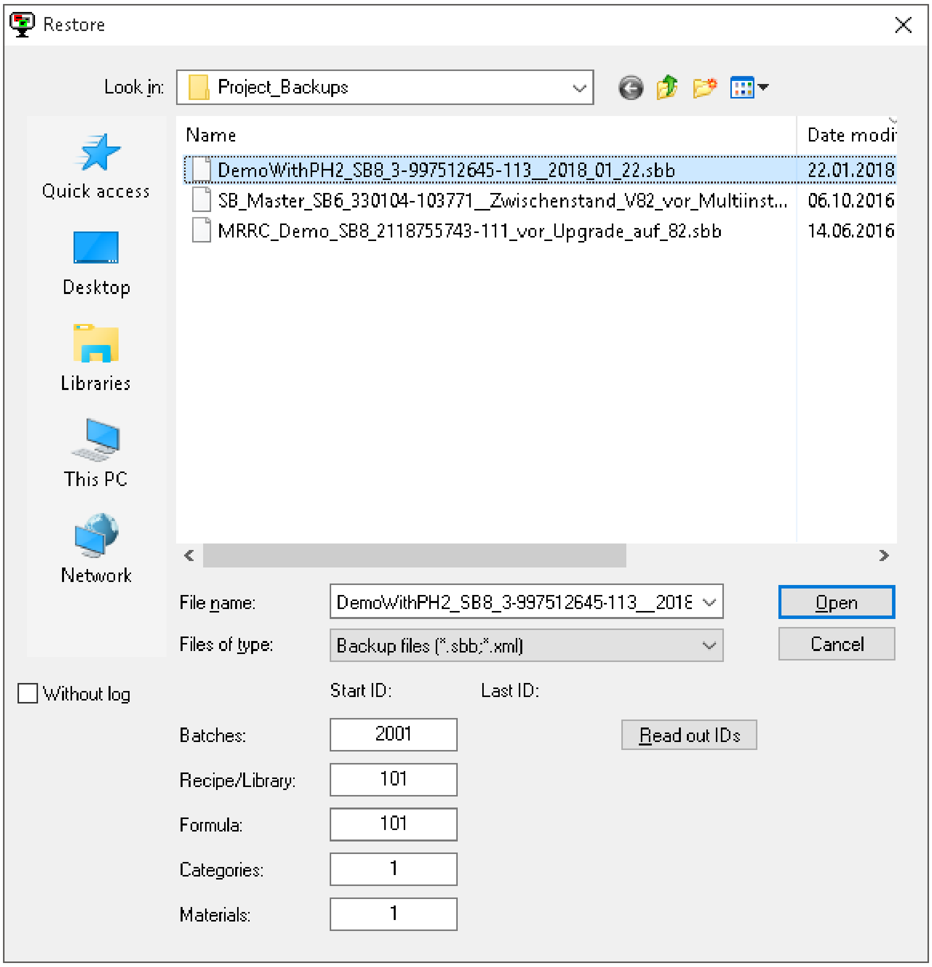
Project-specific adaptations

Project-specific adaptations to the system that are not stored with the project file must be restored.

Backup/restore for the SIMATIC BATCH database

When a data backup of the SIMATIC BATCH database is read, a start batch ID can be assigned; this prevents batch IDs being assigned more than once.

This dialog box also specifies the import of the corresponding log book.



Restore

Look in: Project_Backups

Name	Date modi
DemoWithPH2_SB8_3-997512645-113__2018_01_22.sbb	22.01.2018
SB_Master_SB6_330104-103771__Zwischenstand_V82_vor_Multiinst...	06.10.2016
MRRC_Demo_SB8_2118755743-111_vor_Upgrade_auf_82.sbb	14.06.2016

File name: DemoWithPH2_SB8_3-997512645-113__2018

Files of type: Backup files (*.sbb;*.xml)

□ Without log

	Start ID:	Last ID:
Batches:	2001	
Recipe/Library:	101	
Formula:	101	
Categories:	1	
Materials:	1	

System Updates and Migration 10

10.1 General procedure

It is essential that system software updates for a validated plant are agreed upon with the user or initiated by them. 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 164)", this roughly means the following steps:

- Describe the planned change
- Effect on functions / plant units / documentation, for example, including the system description of the new and modified functions in the readme file/release notes for system updates
- Effect on readability and availability of archived data
- Assessment of the risks for the overall process and the validated status
- Define the tests which need to be performed to obtain validated status, based on the risk assessment
- Approve/reject the change (in accordance with defined responsibilities)
- Updating of existing system description and preparation of the test documents
- Perform data backup before update
- Make the change (following plant release)
- Accompanying documentation of the activities performed
- Perform and document the necessary tests (verification)
- Perform new data backup, possibly including system image

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

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

10.2 Updating the system software

Updates of the system software may be, for example:

- SIMATIC PCS 7 updates, service packs and new versions
- Updates of standard software such as Microsoft Office or virus scanners
- Operating system updates

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

When there is an update of the system software, it may be necessary to migrate or convert configuration data of the project of the older version, see chapter "Migration of the application software (Page 170)".

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

See also

- FAQ "Information on PCS 7 software update", Online Support under entry ID 39980937 (https://support.industry.siemens.com/cs/ww/en/view/39980937)
- Manual "PCS 7 Compendium Part D", chapter 3, Online Support under entry ID 109808463 (https://support.industry.siemens.com/cs/ww/en/view/109808463)
- FAQ "Microsoft security updates", Online Support under entry ID 18490004 (https://support.industry.siemens.com/cs/ww/en/view/18490004)
- GAMP 5 Guide, Appendix S4 "Patch and update management"
- GAMP Good Practice Guide "IT Infrastructure" 2nd Edition, chapter 13

Note

The SIMATIC Industry Support (http://support.industry.siemens.com) provides support for software updates and project migration.

10.3 Migration of the application software

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

Siemens offers **optimized migration solutions** for the transition to SIMATIC PCS 7.

This means that both users of previous Siemens control systems and of third-party control systems can utilize the benefits of Totally Integrated Automation in their processes, see "Migration to PCS 7" on the internet (http://w3.siemens.com/mcms/process-control-systems/en/simatic-pcs7-migration/Pages/simatic-pcs7-migration.aspx).

A customized migration strategy is designed, taking into account the necessary qualification measures and based on a system analysis, risk analysis, and the relevant general conditions (existing installed base, scheduled plant shutdown periods, etc.). In so doing, the activities for the system update described in chapter "General procedure (Page 169)" must also be taken into consideration.

Technical understanding of the individual steps, whether manual or automated, as well as the consideration of possible error scenarios are the basic requirements for a successful and efficient validation strategy. It is therefore specially important to involve the appropriate expert specialists in the planning process.

See also

- GAMP 5 Guide, Appendix D7 "Data Migration"
- GAMP Good Practice Guide "Operation of GxP Computerized Systems", chapter 17 "Data Migration"

10.4 Validation effort for migration

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

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

- Change request of the operator,
  see chapter "Operational change control (Page 164)"
- Migration plan or update plan
- Checklist for installation / migration
- Test specification to ensure functionality after update
- Test results together with attachments and deviations
- Final report

Test points in the verification

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

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

The steps should be taken into consideration in accordance with chapter "General procedure (Page 169)".

Note

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

Abbreviations

A

Abbreviation	Description
AS	Automation Station
CFC	Continuous Function Chart
CFR	Code of Federal Regulations (USA)
CM	Control Module
CMT	Control Module Type
CSV	File format; but also refers to Computerized System Validation
DCS	Distributed Control System
DS	Design Specification
EM	Equipment Module
EMT	Equipment Module Type
EPH	Equipment Phase
EPHT	Equipment Phase Type
ES	Engineering Station
FAQ	Frequently Asked Question
FAT	Factory Acceptance Test
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
IEA	Import/Export Assistant
IQ	Installation Qualification
OLE	Object Linking and Embedding
OPC	Open Platform Communications
OS	Operator Station
PAA	Plant Automation Accelerator
P&ID	Piping and Instrumentation Diagram
SAT	Site Acceptance Test
SDS	Software Design Specification
SFC	Sequential Function Chart
SMDS	Software Module Design Specification
SMMC	SIMATIC Management Console
SOP	Standard Operating Procedure
SSC	SIMATIC Security Control
URS	User Requirements Specification
UPS	Uninterruptible Power Supply

Abbreviation	Description
UTC	Universal Time Coordinated
VPN	Virtual Private Network
VXM	Version Cross Manager

Index

Get more information

Siemens AG
Digital Industries
Pharmaceutical and Life Science Industry
Siemensallee 84
76187 Karlsruhe, Germany

PDF (A5E42888188-AB)
Produced in Germany

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

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