

GMP Engineering Manual Edition 04/2008



**SIMATIC PCS 7 V7.0**  
Guidelines for Implementing  
Automation Projects  
in a GMP Environment

simatic pcs 7  
DOCUMENTATION ]

**SIEMENS**

## SIMATIC PCS 7 V7.0

## GMP - Engineering Manual

**Guide to implementing  
automation projects  
in a GMP environment**

Introduction

Table of Contents

---

Configuring Systems in the GMP Environment	<b>1</b>
---	----------

---

Requirements of Computer Systems in the GMP Environment	<b>2</b>
---	----------

---

System Specification	<b>3</b>
----------------------	----------

---

System Installation	<b>4</b>
---------------------	----------

---

Project Settings and Definitions	<b>5</b>
-------------------------------------	----------

---

Creating Application Software	<b>6</b>
-------------------------------	----------

---

Support during Qualification	<b>7</b>
------------------------------	----------

---

Operation, Service and Maintenance	<b>8</b>
---------------------------------------	----------

---

System Updates and Migrating	<b>9</b>
---------------------------------	----------

---

Index

## **Safety-Related Notices**

Notices that you should observe to ensure your own personal safety and to avoid damage to property and equipment can be found in the relevant technical manuals. The safety of pharmaceutical products of prime importance to the pharmacist must be evaluated by the pharmaceutical company itself. This document provides information on this topic.

## **Qualified Personnel**

Only **qualified personnel** should be allowed to install and work on this equipment. Qualified persons are defined as persons who are authorized to commission, to ground, and to tag circuits, equipment, and systems in accordance with established safety practices and standards.

## **Trademarks**

SIMATIC®, SIMATIC HMI®, SIMATIC IT® and SIMATIC NET® are registered trademarks of Siemens AG.

Third parties using for their own purposes any other names in this document which refer to trademarks might infringe upon the rights of the trademark owners.

# Introduction

## Purpose of this manual

This manual describes what is required from the pharmaceutical, regulatory viewpoint for Good Manufacturing Practice (GMP), of the computer system, the software and the procedure for configuring SIMATIC PCS 7. The relationship between the requirements and system build is explained based on practical examples.

## Intended audience

This manual is intended for all plant operators, those responsible for control system designs for specific industries, project managers and programmers, servicing and maintenance personnel who use the process control technology in the GMP environment. It describes solutions for implementing automation projects with SIMATIC PCS 7 in situations where the principles of GMP are mandatory.

## Required basic knowledge

Basic knowledge of SIMATIC PCS 7 is required to understand this manual. Knowledge of GMP as practiced in the pharmaceutical industry is also an advantage.

## Disclaimer

This manual contains instructions for system users and programmers for integrating SIMATIC PCS 7 into the GMP environment. It covers validation and takes into account special aspects such as the requirements of FDA 21 CFR Part 11.

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

## Validity of the manual

The information in this manual applies to SIMATIC PCS 7 V7.0 incl. SP1. The components investigated are PCS 7-ES, PCS 7-OS, SIMATIC BATCH as well as the options Central Archive Server and StoragePlus. Refer to the CD-ROM catalog CA01 for information about the exact compatibility with the individual components. The CD-ROM catalog is available online at: [www.siemens.com/automation/ca01](http://www.siemens.com/automation/ca01).

## Position in the information landscape

The system documentation of the SIMATIC PCS 7 is an integral part of the SIMATIC PCS 7 system software. It is available to every user as online help (HTML help) or as electronic documentation in Acrobat Reader format (PDF):

You can find the electronic manuals for SIMATIC PCS 7 V7.0 SP1 on the PCS 7 Toolset DVD.

## Structure of the manual

This manual supplements the existing SIMATIC PCS 7 manuals. The guidelines are not only useful during configuration; they also provide an overview of the requirements for configuration and what is expected of computer systems in a GMP environment.

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

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

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

In the appendix of this manual, you will find an index listing all the important terms.

## Conventions

The following conventions are used in this manual.

Activities involving several steps are numbered in the order in which the activities should be performed.

Procedures involving only a few steps are indicated by a bullet (•).

References to other manuals are shown in bold italic.

## Additional support

If, once you have read the manual, you have any questions about the products described in it, please contact your local Siemens representative.

You will find information on who to contact at:

<http://www.siemens.com/automation/partner>

You will find a guide to the technical documentation we offer for individual SIMATIC products and systems at:

<http://www.siemens.de/simatic-tech-doku-portal>

The online catalog and ordering system are available at:

<http://mall.automation.siemens.com/>

If you have questions on the manual, please contact the A&D Competence Center Pharma:

- E-mail: [pharma.aud@siemens.com](mailto:pharma.aud@siemens.com)
- Fax: + 49 721 595 6930

Additional information about the products, systems and services from Siemens for the pharmaceutical industry can be found at:

<http://www.siemens.com/pharma>

## Training centers

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

- Phone: + 49 911 895 3200
- Internet: <http://www.sitrain.com>

## Technical support

You can reach the technical support for all A&D products

- Using the Support Request form on the web:  
<http://www.siemens.de/automation/support-request>
- Phone: + 49 180 5050 222
- Fax: + 49 180 5050 223

You can find additional information about our technical support online at  
<http://www.siemens.de/automation/service>

## **Online service & support**

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

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

There you can find:

- The Newsletter, which provides the latest information on your products
- The right documents for you, using our Service & Support search engine
- A forum where users and experts from all over the world exchange experiences
- Your local Automation & Drives representative
- Information about on-site services, repairs, spare parts. Much more can be found on our "Services" pages.

# Table of Contents

<b>Table of Contents</b>		<b>vii</b>
<b>1</b>	<b>Configuring Systems in the GMP Environment</b>	<b>1</b>
1.1	Life Cycle Model .....	1
1.2	Regulations, Guidelines and Recommendations .....	6
1.3	Responsibilities .....	8
1.4	Approval and change procedure .....	8
<b>2</b>	<b>Requirements of Computer Systems in the GMP Environment</b>	<b>9</b>
2.1	Hardware categorization .....	9
2.2	Software categorization .....	10
2.3	Configuration Management .....	10
2.3.1	Configuration Identification .....	11
2.3.2	Configuration Control .....	11
2.4	Software creation .....	12
2.4.1	Use of typicals for programming .....	12
2.4.2	Identifying software modules/typicals .....	12
2.4.3	Changing software modules/typicals .....	12
2.5	Access Protection and User Management .....	13
2.5.1	Applying access protection to a system .....	13
2.5.2	User ID and password requirements .....	14
2.5.3	Case sensitivity Smart Cards and Biometric Systems .....	14
2.6	Electronic signatures .....	15
2.6.1	Conventional electronic signatures .....	15
2.6.2	Electronic signatures based on biometrics .....	16
2.6.3	Security measures for user ID / password .....	16
2.7	Audit Trail .....	16
2.8	Time synchronization .....	17
2.9	Archiving Data .....	17
2.10	Reporting batch data .....	18
2.10.1	Components of batch documentation .....	18
2.10.2	Components of the manufacturing Log .....	19
2.10.3	The uses of electronic batch data .....	19
2.10.4	Requirements on electronic records .....	20
2.11	Data backup .....	21
2.11.1	Backup of application software .....	21
2.11.2	Backup of process data .....	23
2.12	Retrieving archived data .....	23
2.13	Use of third-party components .....	24



<b>3</b>	<b>System Specification</b>	<b>25</b>
3.1	Specification of System Hardware.....	26
3.1.1	Selecting Hardware Components.....	26
3.1.2	Hardware Specification.....	27
3.1.3	Hardware Solutions for Special Automation Tasks .....	27
3.2	Security of the Plant Network .....	28
3.3	Specification of Basic Software .....	29
3.3.1	Operating System .....	29
3.3.2	Basic Software for User Administration .....	29
3.3.3	Engineering System Software Components.....	29
3.3.4	HMI Level Software Components.....	31
3.3.5	SIMATIC BATCH Basics and Options.....	33
3.4	SIMATIC Additional Software .....	34
3.4.1	SIMATIC PCS 7 Add-Ons.....	34
3.4.2	Long-Term Archiving with StoragePlus .....	34
3.4.3	Long-Term Archiving with the Central Archive Server (CAS).....	34
3.5	Application Software Specifications.....	35
3.6	Utilities and Drivers.....	36
3.6.1	Printer Drivers.....	36
3.6.2	Virus Scanners .....	36
3.6.3	Image & Partition Tools .....	36
<b>4</b>	<b>System Installation</b>	<b>37</b>
4.1	Installing the Operating System.....	37
4.2	Installing PCS 7 .....	37
4.3	Setting Up User Administration .....	38
4.3.1	User Administration on the Operating System Level.....	38
4.3.2	Security Settings.....	39
4.3.3	Managing SIMATIC User Groups.....	41
4.3.4	Configuring SIMATIC Logon.....	42
4.3.5	Access Protection .....	43
4.4	Administration of User Rights .....	44
4.4.1	Rights Management on the ES.....	44
4.4.2	Rights Management on the OS .....	47
4.4.3	Rights Management in SIMATIC BATCH.....	48
4.5	Configuring Access Protection .....	50
4.5.1	Configuration Settings in Windows.....	51
4.5.2	Configuration Settings on SIMATIC PCS 7 OS.....	52
4.5.3	Secure Configuration .....	52
4.6	Information Security.....	53
4.6.1	SIMATIC Security Control (SSC).....	53
4.6.2	SCALANCE S.....	53
<b>5</b>	<b>Project Settings and Definitions</b>	<b>55</b>
5.1	Multiproject Setup .....	55
5.2	Referenced OS Stations.....	57
5.3	Using the Master Data Library.....	58
5.3.1	Synchronizing Shared Declarations .....	59
5.3.2	Synchronizing SFC Types .....	60
5.3.3	Synchronizing the Plant Hierarchy .....	61
5.4	Views .....	62
5.5	SIMATIC NET .....	62
5.5.1	Configuring SIMATIC NET.....	62
5.5.2	Plant Bus and Terminal Bus .....	63
5.5.3	PROFIBUS .....	63
5.5.4	SIMATIC PDM .....	68
5.5.5	FOUNDATION Fieldbus (FF).....	70

5.6	OS Project Editor .....	71
5.7	Time Synchronization .....	72
5.8	Configuration Management .....	74
5.9	Versioning Software Elements .....	75
5.9.1	Versioning AS Elements in PCS 7 .....	75
5.9.2	Versioning OS Elements in PCS 7 .....	79
5.9.3	Further Information on Versioning .....	81
<b>6</b>	<b>Creating Application Software .....</b>	<b>83</b>
6.1	Software Modules, Types, and Typicals .....	84
6.1.1	Modules and Typicals in PCS 7 .....	84
6.1.2	Example of a Process Tag Type .....	86
6.1.3	Automatic Generation of Block Icons .....	86
6.2	Bulk Engineering with the IEA .....	89
6.3	Creating Process Diagrams .....	90
6.4	User-Specific Blocks and Scripts .....	91
6.5	Interfaces to PCS 7 .....	92
6.5.1	PCS 7 OS Web Option .....	92
6.5.2	Open PCS 7 .....	93
6.5.3	SIMATIC BATCH API .....	94
6.6	Integrating SIMATIC BATCH .....	95
6.6.1	Batch Definition of Terms .....	95
6.6.2	Conformity with the ISA-88.01 Standard .....	95
6.6.3	ISA-88.01 - Software Model SIMATIC PCS 7 .....	96
6.6.4	Implementing the ISA-88.01 Concept .....	97
6.6.5	Configuring SIMATIC BATCH .....	98
6.6.6	Creating Batch Reports .....	100
6.7	SIMATIC Route Control .....	102
6.8	Alarm Management .....	104
6.8.1	Specification .....	104
6.8.2	Event-signaling Classes .....	104
6.8.3	Priorities .....	105
6.8.4	Suppressing, Filtering, Hiding .....	106
6.8.5	Monitoring PCS 7 Components .....	108
6.8.6	Monitoring Connected Systems .....	108
6.9	Audit Trail and Change Control .....	109
6.9.1	PCS 7 ES .....	109
6.9.2	PCS 7 OS .....	112
6.9.3	SIMATIC BATCH .....	113
6.10	Configuration for Electronic Signatures .....	116
6.10.1	Electronic Signatures in SIMATIC BATCH .....	116
6.10.2	Electronic Signatures on PCS 7 OS .....	118
6.10.3	Electronic Signatures on PCS 7 ES .....	118
6.11	Data Backup .....	119
6.11.1	Backing Up the System Configuration .....	119
6.11.2	Backing Up the Application Software .....	120
6.12	Recording and Archiving Data Electronically .....	121
6.12.1	Specifying the Data to be Archived .....	121
6.12.2	Setting Up Process Value Archives .....	122
6.12.3	Long-Term Archiving with the Central Archive Server (CAS) .....	123
6.12.4	Long-Term Archiving With StoragePlus .....	127
6.13	Uninterruptible Power Supply (UPS) .....	130
6.13.1	Configuring the UPS .....	131
6.13.2	UPS Configuration over Digital Inputs .....	132
6.13.3	MASTERGUARD UPS Systems .....	133

<b>7</b>	<b>Support during Qualification</b>	<b>135</b>
7.1	Qualification Planning .....	136
7.2	Qualification of Hardware .....	136
7.3	Qualification of Software .....	138
7.3.1	Software Categorization according to GAMP Guide .....	138
7.3.2	Qualification of Standard Software .....	139
7.3.3	Qualification of the Application Software .....	142
7.3.4	Simulation for Test Mode .....	143
7.4	Configuration Control .....	144
7.4.1	Versioning Projects with "Version Trail" .....	144
7.4.2	Change Control with "Version Cross Manager" (VXM) .....	147
<b>8</b>	<b>Operation, Service and Maintenance</b>	<b>149</b>
8.1	Asset Management .....	149
8.2	Change Control during Operation .....	151
8.3	Remote Maintenance .....	151
8.4	Date Retrieval .....	152
<b>9</b>	<b>System Updates and Migrating</b>	<b>153</b>
9.1	Updates, Service Packs and Hotfixes .....	153
9.2	Migrating to PCS 7 .....	154
	<b>Index</b>	<b>155</b>

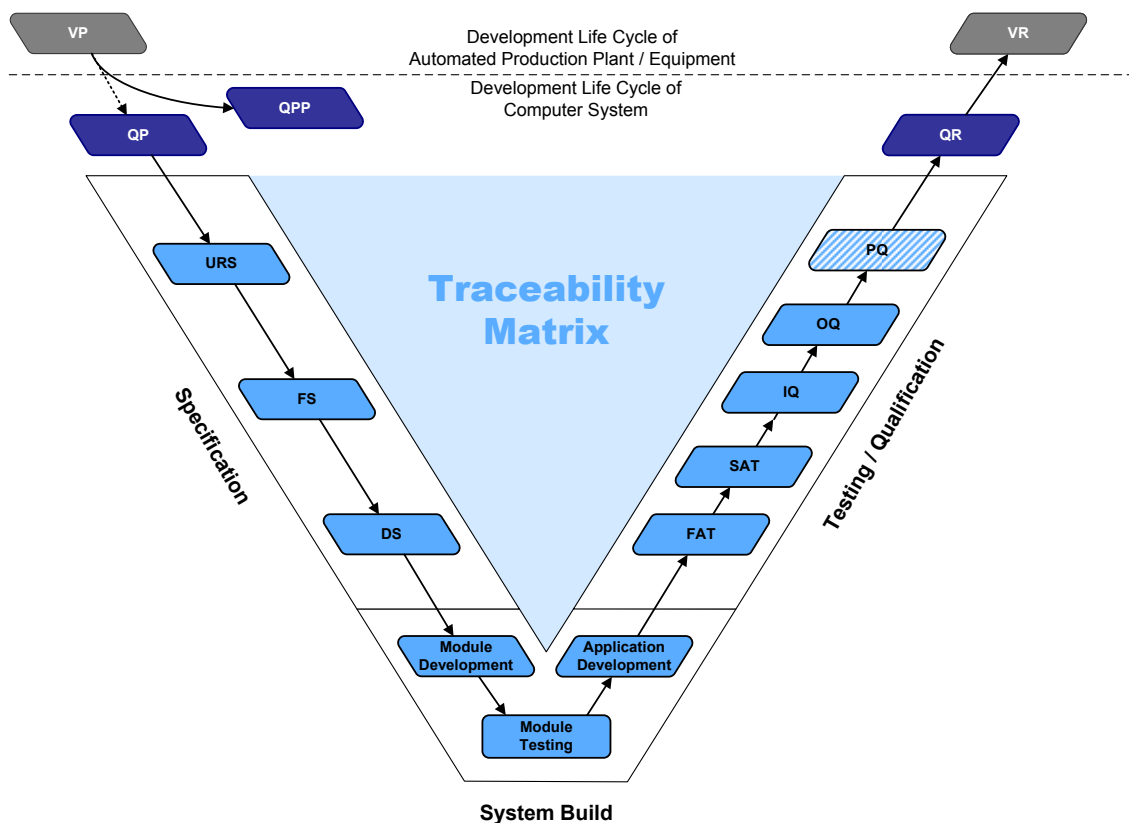
# 1 Configuring Systems in the GMP Environment

The availability of approved specifications, such as User Requirements Specification (URS) and Functional Specification (FS), is a prerequisite for the configuration of computer systems in the GMP environment. Requirements contained in standards, recommendations, and guidelines must be observed when creating these specifications. This chapter deals with the most important of these sets of regulations as well as various specifications (URS, FS, DS).

## 1.1 Life Cycle Model

A central component of Good Engineering Practice (GEP) is the application of a recognized project methodology, based on a defined life cycle. The aim is to deliver a solution that meets the relevant requirements and is also cost-effective.

The figure below shows the development life cycle model used in this manual. It is based on the recommendations of the GAMP Guide for Validation of Automated Systems. It begins with the planning phase of a project and ends with the start of pharmaceutical production following completion of qualification and validation.



## Legend for the Life Cycle Model

Abbreviation	Description
VP	Validation Plan
QP	Qualification Plan
QPP	Quality and Project Plan
URS	User Requirements Specification
FS	Functional Specification
DS	Design Specification
FAT	Factory Acceptance Test
SAT	Site Acceptance Test
IQ	Installation Qualification
OQ	Operational Qualification
PQ	Performance Qualification
QR	Qualification Report
VR	Validation Report

### Validation Plan

The Validation Plan (VP) specifies the overall strategy and specifies the parties responsible for the validation of a system in its operational environment [PDA, GAMP 4].

In the case of complex plants (for example a production line with several process cells and computer systems), there may also be a master validation plan (MVP) as well as VPs valid only for specific process cells and systems.

See also **GAMP 4**, Appendix M1 "Guideline for Validation Planning".

### Qualification Plan

In contrast to the Validation Plan, a Qualification Plan (QP) describes the qualification activities in detail. It defines the tests to be performed and indicates the dependencies.

The Qualification Plan follows a Validation Plan. Due to the similar contents of both documents, it is possible to combine the QP and the QPP.

## Quality and Project Plan

The Quality and Project Plan (QPP) defines the scope of and procedures relating to project and quality management, with document and change control procedures, for example, being specified. The life cycle is defined in such a way in the QPP that it not only includes project phases which are relevant for validation, but also other organizational relationships (e.g. different time schedules from the various sections, for example).

Due to their similar structures and contents, a combination of the QPP and QP is possible.

See also **GAMP 4**, Appendix M6 "Guideline for Quality and Project Planning".

## Specification

The specification phase starts with the creation of the URS. As a rule, the URS is created by the user and describes the requirements which the system has to meet. Once the URS has been created, an FS is created, usually by the supplier. The FS describes the requirements defined in the URS more precisely on a functional level. The subsequent DS contains detailed requirements as regards system build.

The functional and design specifications both form the basis for later qualification and validation tests. The following issues also have to be addressed during the function and design specification phases:

- Software structure
- Programming / coding standards
- Naming conventions
- File naming convention

## User requirements specification (URS)

The URS describes the requirements the system has to meet from the user's point of view. The URS is generally created by the system user and it is system independent; its creation can possibly be supported by the system supplier.

It is the basis of all subsequent specifications.

See also **GAMP 4**, Appendix D1 "Example Procedure for the Production of a URS".

## Functional Specification (FS)

As a rule, the FS is created by the system supplier, occasionally in collaboration with the end user. It describes in detail the functions of the system, based on the URS. The approved FS is the basis for creating detailed specifications.

See also **GAMP 4**, Appendix D2 "Example Procedure for the Production of a FS".

## Design Specification (DS)

The Design Specification is usually created by the system supplier. It is based on the FS and expands this with detailed descriptions, for example, of the hardware and software to be used, process tag lists, etc. These single specification areas can also be divided into several documents, for example:

- Hardware Design Specification (HDS) incl. description of the network structure
- Software Module Design Specification (SMDS) for typicals
- Software Design Specification (SDS)
- Further documents like tag list, I/O list, parameter list, P&I diagrams, etc.

See also **GAMP 4**, Appendix D3 "Example Procedure for the Production of a Hardware Design Specification" and Appendix D4 "Example Procedure for the Production of Software Design Specifications and Software Module Design Specifications".

## System Build

The system is implemented in accordance with the Design Specification during the system build stage. Along with the procedures defined in the QPP and additional guidelines (coding standards, naming conventions, and data backups, for example), change management, which aims to enable changes to and deviations from the original specifications to be traced, plays an important role.

See also **GAMP 4**, Appendix M8 "Guideline for Project Change Control" and Appendix M10 "Guideline for Document Management".

## FAT

Once the system build steps have been completed, a Factory Acceptance Test (FAT) is often carried out on the supplier's premises and documented, enabling any programming errors to be identified and remedied prior to delivery.

The aim of the FAT is the acceptance of the customer for system delivery in its tested state.

## SAT

The Site Acceptance Test (SAT) shows that a computer system works within its target operating environment with interfaces to the instrumentation and plant sections according to the specification. Depending on the project, the SAT can be combined with commissioning, IQ and/or OQ.

## **Test phase / Qualification**

The FAT is followed by technical commissioning (commissioning phase). This involves installing the system at the system operator's premises along with the application software created, followed by technical commissioning, testing, and qualification.

The commissioning and qualification phases can follow on from one another or can be combined. To save time and money, it is recommended that commissioning and qualification activities are coordinated.

The test planning should therefore be created in good time so that it is possible to check whether or not tests undertaken beforehand during FAT or SAT need to be repeated during qualification. In this case, the documented FAT / SAT tests become part of the qualification documentation.

When test documents are created, tests and acceptance criteria must be clearly described.

## **Qualification Report**

The Qualification Report (QR) summarizes the results of the tests performed, based on the Qualification Plan, and confirms that the qualification phases have been completed successfully.

## **Validation Report**

The Validation Report (VR) sums up the results of the individual validation steps and confirms the validated status of the system. The creation of both the Validation Plan and the Validation Report is the responsibility of the customer.



## 1.2 Regulations, Guidelines and Recommendations

In addition to the effective laws and regulations, recommendations and guidelines of various organizations have to be taken into account when configuring computer systems in the GMP environment. These are usually based on general guidelines and regulations, such as Code of Federal Regulations Title 21 (21 CFR) of the US Food and Drug Administration (FDA) or the EU GMP Guide Annex 11.

Regulation / Guideline	Author / organization	Title	Regulation / Recommendation	Scope
21 CFR Part 11	US FDA	Electronic records, electronic signature	Law, regulation	Manufacturers and importers of pharmaceutical products for the US market
21 CFR Part 210	US FDA	Current good manufacturing practice in manufacturing, processing, packing, or holding of drugs; general		
21 CFR Part 211	US FDA	Current good manufacturing practice for finished pharmaceuticals		
Annex 11 of the EU Guidelines for GMP	European Commission Directorate General III	Computerised Systems	Guideline	Europe
Annex 18 of the EU Guidelines for GMP	European Commission Directorate General III	Good Manufacturing Practice for Active Pharmaceutical Ingredients	Guideline	Europe
GAMP 4	ISPE	GAMP Guide for Validation of Automated Systems	Guide	Worldwide
GAMP Good Practice Guide	ISPE	Validation of Process Control Systems	Recommendation	Worldwide
NAMUR NE 71	NAMUR	Operation and Maintenance of Validated Systems	Recommendation	Europe

### Note

This manual is based on the requirements of **GAMP 4** and **US 21 CFR Part 11**.

## **Code of Federal Regulations Title 21 (21 CFR), Food and Drugs**

Code of Federal Regulations Title 21 is comprised of different Parts, such as Parts 11, 210, and 211. Part 11 is of particular significance for computerized systems (and is known as 21 CFR Part 11). This Part deals with electronic records and electronic signatures.

## **Annex 11 of the EU Guidelines to GMP**

Annex 11 of the EU Guidelines to GMP contains 19 points which describe the configuration requirements, operation, and change control of computer systems in the GMP environment. An interpretation of Annex 11 can be found in the GAMP 4 Guide for Validation of Automated Systems in the form of an APV (International Association for Pharmaceutical Technology) guideline.

## **Annex 18 of the EU Guidelines to GMP**

Annex 18 of the EU Guidelines to GMP deals with good manufacturing practice (GMP) for active pharmaceutical ingredients (API). It is designed to be used as a GMP guide when manufacturing active pharmaceutical ingredients in the context of a suitable quality management system. Section 5 of Annex 18 deals with process equipment and its use.

## **GAMP Guide for Validation of Automated Systems**

The GAMP (Good Automated Manufacturing Practice) Guide for Validation of Automated Systems was compiled to be used as a recommendation for suppliers and a guide for the users of computer systems in the pharmaceutical manufacturing industry. Version GAMP 4 was published in December 2001.

## **GAMP Good Practice Guide - Validation of Process Control Systems**

In addition to the recommendations of the GAMP Guide, there are some Good Practice Guides dealing with special topics. This one mentioned here gives recommendations how to validate Process Control Systems (DCS).

## **NAMUR recommendations**

NAMUR recommendations are reports of the experience that were produced by the "Process Control Systems Special Interest Group of the Chemical and Pharmaceutical Industry" for optional use by its members. They should not be viewed as standards or guidelines. The NAMUR recommendations below are of particular interest for the configuration and use of computer systems in the GMP environment:

- NE 71 "Operation and Maintenance of Validated Systems"

## 1.3 Responsibilities

Responsibilities for the activities included in the individual life cycle stages must be defined when configuring computer systems in the GMP environment and creating corresponding specifications. As this definition is usually laid down on a customer- and project-specific basis and requires a contractual agreement, it is recommended that the definition is integrated into the Quality and Project Plan. See also **GAMP 4**, Appendix M2.

## 1.4 Approval and change procedure

When new systems requiring validation are set up or when existing systems requiring validation are changed, the top priority is to achieve or retain validated status.

### Setting up new systems

If a new system is set up, document approval and the transitions between life cycle stages are defined prior to commencement of the project. This is usually carried out in conjunction with the definition of responsibilities contained in the Quality and Project Plan. A life cycle like the one described in Chapter 1.1 “Life Cycle Model” is used.

### Changing validated systems

Changes to an existing, validated system are regulated as per the company's Change Control procedures. Before any changes are carried out they must be described, potential consequences must be identified, and associated steps (performing tests, updating as-built documentation, for example) must be defined. Once final approval has been received, the planned change is carried out, as are the defined steps.

If comprehensive changes are needed, a life cycle similar to the one shown in this manual may be used if required.

## 2 Requirements of Computer Systems in the GMP Environment

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

### 2.1 Hardware categorization

A system's hardware components are assigned to one of two hardware categories in accordance with the **GAMP 4** Guide, Appendix M4. The hardware categories are listed below:

#### Category 1, standard hardware

Category 1, standard hardware includes established, commercially-available hardware components. This type of hardware is also subject to the relevant quality and testing mechanisms.

The hardware is accepted and documented by means of an IQ test.

#### Category 2, customized hardware

The functionality of such hardware must be specified, then checked and documented in detail by means of appropriate, documented tests.

## 2.2 Software categorization

According to the *GAMP Guide for Validation of Automated Systems*, the software components of a system are assigned to different software categories. This ranges from commercially available standard software packages, which are only to be installed, to software written via free coding.

For commercially available standard software packages the name and the version number are documented and checked in a documented test. Customer specific requirements like access protection, alarms and event management, calculations, etc. are to be specified and also be checked in a documented test.

In addition to the above mentioned, project specific configurations of configurable software packages are to be specified and checked in a documented test.

A detailed software specification is to be created for software especially developed for special customer needs. Besides of the functional tests, also structural software tests (code reviews) should be conducted.

Hence, test effort for software of higher software categories is much higher than for lower software categories, and the total test effort can be reduced by using standardized software components as far as possible.

## 2.3 Configuration Management

The **GAMP 4** Guide defines configuration management as the process which needs to be followed in order to precisely define an automated system at any point during its life cycle, from initial development right through to decommissioning of the system.

Configuration management involves using administrative and technical procedures in order to:

- Identify and define basic system components and to specify them in general
- Control changes to and approvals of elements
- Record and document element statuses and modifications
- Ensure elements are complete, consistent, and correct
- Control the storage, treatment, and delivery of elements.

Configuration management comprises the following activities:

- Configuration identification (what is to be kept under control)
- Configuration control (how the control is performed)
- Configuration status report (how the control is documented)
- Configuration evaluation (how the control is verified)

This chapter deals with configuration identification and configuration control.

### **2.3.1 Configuration Identification**

Version and change management is only practicable with a suitable configuration environment. Siemens therefore identifies every software and hardware package using a unique product label (Machine-Readable Product Code - MLFB) and version identifier. For the application software, the parts of a computer system that are subject to configuration management must be clearly specified. The system must be divided into configuration elements to this end. These must be defined at an early stage of system build to ensure that a complete list of configuration elements can be created and maintained. Application-specific elements should have a unique ID (name or identification number). The amount of detail required when defining elements is determined by the requirements of the system and the supplier who is developing the application.

### **2.3.2 Configuration Control**

The maintenance of configuration elements must be checked at regular intervals by means of reviews, for example. Here, particular attention must be paid to the change control and the related versioning. Archiving and release of individual configuration items should also be taken into account.

## **Versioning**

To ensure correct change management, the configuration elements must be versioned. The version must be updated each time a change is made.

## **Change Control**

Suitable control mechanisms must be in place during configuration in order to ensure that changes are documented and transparency achieved. The control mechanisms can be described by means of SOPs and must cover the following:

- Software versioning
- Specifications such as programming guidelines, naming conventions, etc.
- Safeguarding of the traceability of changes to program codes
- Unique identification of software and all components contained within

## **2.4 Software creation**

Certain guidelines must be followed during software creation, which should be documented in the Quality and Project Plan (GEP idea). Software creation guidelines can be taken from the *GAMP 4* Guide and from relevant standards and recommendations.

### **2.4.1 Use of typicals for programming**

As shown in Chapter 2.2 “Software categorization” the amount of validation work required increases enormously as you go up through the GAMP software categories. While the validation of lower software categories only calls for the software name and version to be checked, category 5 software validation requires the entire range of functions to be checked and a supplier audit to be performed.

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

### **2.4.2 Identifying software modules/typicals**

During software creation the individual software modules must be assigned a unique name, a version, and a short description of the module. If changes are made to software modules, this must be reflected in the module ID.

### **2.4.3 Changing software modules/typicals**

If changes are made to software modules, this must be noted in the corresponding module ID. As well as incrementing the version identifier, the date of the change and the name of the change initiator must also be included in the software module's ID. If required, the software modules to be changed must be indicated by means of a comment and a reference to the corresponding change request/order. See also Chapter 8.2.

## 2.5 Access Protection and User Management

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

- A combination of unique user ID and password - a description of the configuration can be found in chapters 4.3 and 4.4
- Chip cards in combination with a password
- Biometric systems

The system owner or an employee (administrator) nominated by him controls the assignment and management of user authorizations to ensure that access is suitably protected.

### 2.5.1 Applying access protection to a system

In general, actions which can be executed on a computer system must be protected. Depending on his or her particular field of activities, a user can be assigned various rights. Access to user administration should only be given to the system owner or to specified employees. Recorded electronic data must still be protected against unauthorized access.

An automatic logout function should be installed on the system. The logout time should be agreed and defined with the operator and noted in the FS.



---

#### Note

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

---



## **2.5.2 User ID and password requirements**

### **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:**

A password should usually be a combination of numeric and alphanumeric characters. When defining passwords, the minimum number of characters and the expiry period for the password should be defined. Generally, the password structure is defined on a customer-specific basis. The configuration is described in the chapters 4.3 and 4.4.

Password structure criteria:

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

In order to comply with the Windows guidelines for password complexity, at least three of the criteria listed must be taken into account in the password alongside the minimum length.

## **2.5.3 Case sensitivity Smart Cards and Biometric Systems**

Apart from the traditional methods of identification with a user ID and password, users can also identify themselves with smart cards along with a password/PIN or with biometric systems, such as fingerprint scanners.

## 2.6 Electronic signatures

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

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

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

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

Electronic signatures can be biometrically based or the system can be set up without biometric features.

---

### Note

The regulations found in 21 CFR Part 11, published by the FDA, must be satisfied in the manufacture of all pharmaceutical products and medical devices intended for the US market.

---

### 2.6.1 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.

When owners of signatures want to use their electronic signatures, they must identify themselves with at least two identification components. The exception to this rule is when the owner executes several electronic signatures during one uninterrupted session. In this case, persons executing signatures need to identify themselves with both identification components only when applying the first signature. For the second and subsequent signatures, one unique identification component (password) is then adequate identification.

## 2.6.2 Electronic signatures based on biometrics

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

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

---

### Note

The use of biometric systems is currently considered a secure identification method. Nevertheless, there are reservations about the use of biometric identification characteristics in the pharmaceutical industry (e.g. poor face recognition due to protective clothing covering the face, no fingerprint scans with gloves, the expense involved and the reaction times of retina scans).

---

## 2.6.3 Security measures for user ID / password

The following points must be observed in order to safeguard the security of electronic signatures where user IDs and passwords are used:

- Uniqueness of user ID and password
- Monitored output of user IDs
- Permissions retracted if user ID/password is lost or found to be insecure or compromised
- Security precautions used to prevent the unauthorized use of user ID / password or to report any misuse
- Personnel trained and provided with written evidence of such training

## 2.7 Audit Trail

The Audit Trail is a control mechanism of the system that allows entries or modifications of data to be traced back. A secure Audit Trail is particularly important as regards the creation, modification, or deletion of GMP-relevant electronic records.

In this case, the Audit Trail must document all changes or actions performed, together with the corresponding date and time. The typical content of an Audit Trail must be specified and must cover "who" has changed "what" and "when" (old value/new value).

The Audit Trail records themselves needs to be archived for a defined time period according to the stipulations in the specification documents.

There must be adequate hard disk space to ensure the entire Audit Trail to be stored until the next transfer to an external data medium.

Systems which provide adequate data security must be used (e.g. redundant systems, standby systems, mirrored hard disks based on RAID 1).

## 2.8 Time synchronization

A consistent time reference (including a time zone reference) must be guaranteed within a system, in order to be able to assign a unique time stamp for archiving messages, alarms, etc.

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

## 2.9 Archiving Data

Archiving (electronically) means the permanent storage of electronic data and records of a computer system in a long-term storage system.<sup>1</sup>

The customer is responsible for the definition of processes and regular checks involved in storing electronic data.

Based on the predicate rules (EU Guidelines for GMP, 21 CFR Part 210, 21 CFR Part 211, etc.), the customer must decide how electronic data will be retained and, in particular, which data will be affected by this procedure. This decision should be based on a justified and documented risk assessment that takes into account the significance of the electronic records over the archiving period.

The customer should define the following requirements<sup>2</sup>:

- Whether any archiving is even required for the application in question (backup/restore function may be different from the archive function)
- Required archiving duration for the relevant data, based on legal and commercial requirements
- An archiving procedure containing the restoration capability at any time in the archiving period as well as ensuring data formats, which are easy to migrate

Process values (often in the form of trends), messages (alarms, warnings, etc.), Audit Trails, and maybe other batch data can be archived for SIMATIC systems.

---

<sup>1</sup> "Good Practice and Compliance for Electronic Records and Signatures. Part 1, Good Electronic Records Management". ISPE/PDA 2001.

<sup>2</sup> "Good Practice and Compliance for Electronic Records and Signatures. Part 3, Models for Systems Implementation and Evolution". PDA 2004.

The memory space on a system's data carriers is restricted. Data can be swapped out to external data carriers at regular intervals in order to free up space on these system data carriers.

When migrating or converting the archived data, the integrity of the data must be assured over the entire conversion process.<sup>3</sup>

## **2.10 Reporting batch data**

When producing pharmaceuticals and medical equipment, batch documentation takes on a special significance. For a pharmaceutical manufacturer, methodically created batch documentation is often the only documented evidence within the framework of product liability.

### **2.10.1 Components of batch documentation**

Batch documentation comprises the following:

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

The manufacturing log (or packaging log) has a central significance here and this is defined below:

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

---

<sup>3</sup> "Good Practice and Compliance for Electronic Records and Signatures. Part 3, Models for Systems Implementation and Evolution". PDA 2004.

### **2.10.2 Components of the manufacturing Log**

Mandatory parts of the manufacturing log include:

- Name of the product and number of the produced batch
- Date and time of commencement, significant interim stages and completion of production
- Name of the person responsible for each stage of production
- Initials of the operator involved in each significant production step and, when applicable, the person checking the operations (double-check when weighing materials, for example)
- The batch number and / or the analytical control number and the actual quantities of all constituent materials used
- All relevant processing steps, any unusual events and the major equipment used
- Recordings of in-process controls, including initials of the persons performing them and the results obtained
- The yields of the relevant interim stages
- Information on special problems, including details of any deviation from the manufacturing formula and processing instructions and the signature of the person who authorized the deviation.

### **2.10.3 The uses of electronic batch data**

Since the term "electronic batch record" (acronym: EBR) is not clearly defined in this context, there are two ways of using electronic records in the documentation of pharmaceutical production:

1. The electronic records form part of the batch documentation or
2. The entire manufacturing log is created electronically.

Since all the requirements listed above must be met by an electronic manufacturing log and data from different systems (for example, PCS, laboratory data, remarks by operators) also often needs to be integrated, the situation is often as in case 1.

#### **2.10.4 Requirements on electronic records**

When electronic records are used as part of the batch documentation or even as the manufacturing log itself, the following additional requirements apply (see also EU GMP Guide, Section 4.9; 21 CFR Part 11 Electronic Records, Electronic Signatures):

- 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
- The system must be validated
- Only authorized persons must be able to enter or change data (access protection)
- Changes to data or deletions must be recorded (Audit Trail)
- The relevant electronic records for long-term storage must be archived and protected by appropriate measures and kept available
- If an electronic manufacturing log is used, its structure and contents must match the structure and contents of the manufacturing formula / processing instructions. As an alternative, the manufacturing instructions and log can also be combined in one document

## 2.11 Data backup

In contrast to the archiving of electronic data, data backups are used to create backup copies which allow the system to be restored if the original data or entire system is lost.<sup>4</sup>

The backup procedure must cover the periodic backup of volatile information to avoid total loss of data due to defective system components or inadvertent deletion of data. Backup procedures must be tested to ensure that data is saved correctly. Backup records should be labeled clearly and intelligibly and dated.<sup>5</sup>

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

When backing up electronic data, a distinction is made between software backups (for example application software, partition images) and archive data backups.

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

### 2.11.1 Backup of application software

Software backups have to be created following every software change on a system and must document the system's last valid software version. If parts of the software are modified, it is sufficient to only back up the modified part of the application software. Complete software backups still have to be created at regular intervals, however. If software backups are to be created as part of a software change on an existing system or a system reinstallation, they must be created once the installation has been performed. During the course of the project the software version must be backed up and documented at defined milestones, such as at the end of the FAT (i.e. prior to delivery of the system), once the Installation Qualification (IQ) has been completed, prior to the tests involved in the Operational Qualification (OQ), and, of course, when the system is handed over to the system owner.

Software versions should also be stored in the form of software backups at regular intervals during the creation of new software versions.

Software backups of the application software and configuration parameters must be created.

---

<sup>4</sup> "Good Practice and Compliance for Electronic Records and Signatures. Part 1, Good Electronic Records Management". ISPE/PDA 2001.

<sup>5</sup> "Electronic Records and Electronic Signatures Assessment". Chris Reid & Barbara Mullendore, PDA 2001.



### **Labeling software backups**

According to the *GAMP 4* Guide, the following information about software backups should be provided, both on the label of the backup medium and in a separate log:

- Creation date
- System name
- Software or version name
- Serial number of backup
- Reason for the software backup
- Date of first use
- Date of backup
- Date and signature of the person performing the backup
- Identity of the user

### **Retaining software backups**

At least the two most recent software backups should be retained. For reasons of safety, these should be stored at a different location from the system, for example in a fire compartment separate from the system).

A suitable backup strategy must be defined, based on the frequency with which changes are made to the software.

The data carrier's shelf life should be defined (based on manufacturer documentation, e. g.) and the software backup must be appropriately migrated by copying it to a new data carrier, for example, before this period expires.

### **2.11.2 Backup of process data**

The data stored in computer systems, such as trends, measured values, or interventions, should be backed up to external data carriers at regular intervals. This will minimize the risk of data being lost should a fault occur.

#### **Labeling process data backups**

According to the *GAMP 4* Guide, data backups should be documented either on the label of the backup itself or in a separate report containing the following information:

- System designations
- Software / data designation
- Version and/or software/firmware build number, if available
- Creation date
- Date of first usage
- Consecutive number
- Date of the data backup
- Reason for the data backup
- Identity of the user

#### **Retaining process data backups**

The same guidelines apply as in the chapter about retaining backups in chapter 2.11.1.

Since process data, in contrast to software, is not normally stored in "overlapping" versions, suitable measures must be taken to ensure data integrity.

## **2.12 Retrieving archived data**

Backed up data must be retrievable at all times. Following system updates, care must be taken that the data transferred to archive prior to the update remains compatible.

## 2.13 Use of third-party components

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

Compatibility must also be confirmed when standard hardware and software components provided by other manufacturers are used.

---

### Note

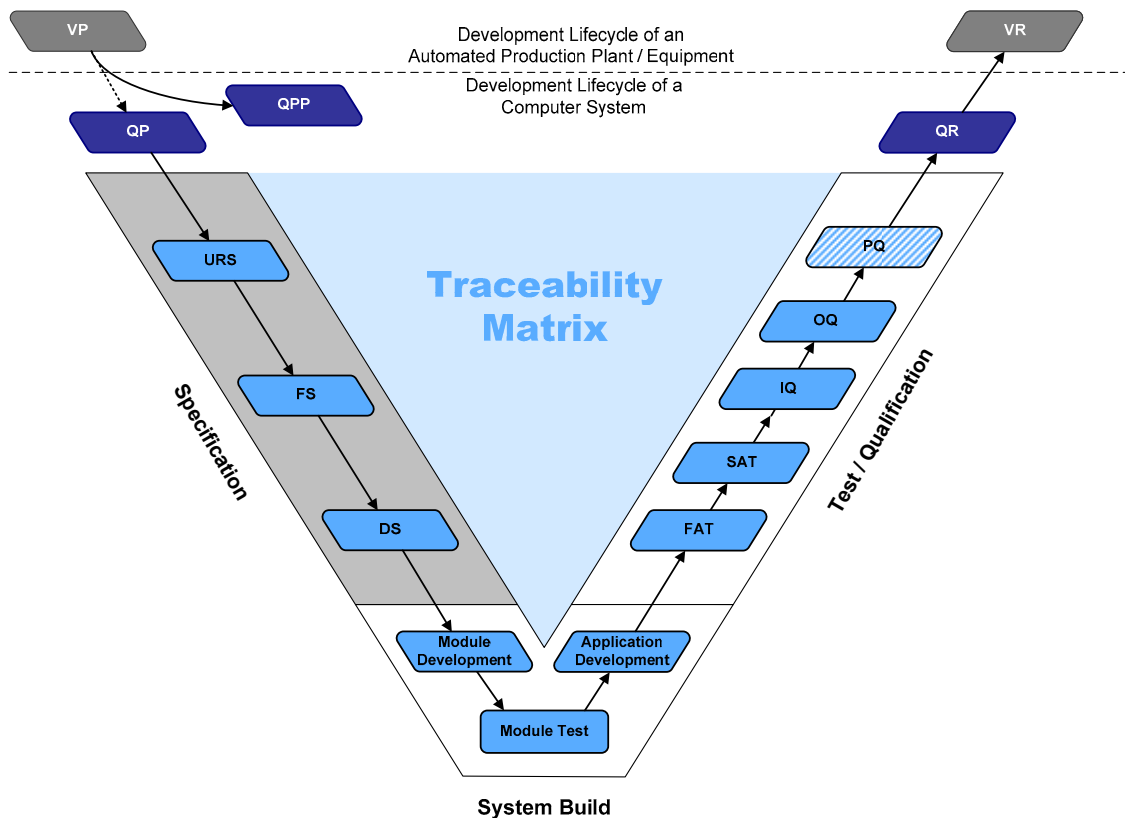
The **GAMP 4** Guide in Appendix M2 contains information on auditing a product supplier.

---

### 3 System Specification

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

In the following graphic the highlighted area at the left-hand side illustrates the phase of the system specification, where the activities of this section belong to.



## 3.1 Specification of System Hardware

### 3.1.1 Selecting Hardware Components

Using hardware components from the PCS 7 catalog ensures that hardware and spare parts will continue to be available in the long term.

In the interests of system availability and data security/integrity, RAID systems of an appropriate class should be used when designing PC components such as ES, OS single-user stations, OS servers, and BATCH servers.

The manual *PCS 7 PC-Configuration and Authorization* also contains information on system configurations.

When a SIMATIC PCS 7 bundle is supplied, the customer receives a PC with all software required for the relevant applications installed (operating system, SIMATIC PCS 7 software, service packages). The components contained in the bundle are not always identical to the products of the same names available on the open market and, as a consequence, the availability of compatible spare parts will differ too. In the case of unreleased system configurations, additional specification and qualification work must be carried out as part of the project and any problems as regards compatibility taken into account.

---

#### Note

Only released hardware from the current PCS 7 catalog should be used; the use of unreleased configurations results in additional qualification work being required.

---

---

#### Note

If PCs are distributed in control cabinets, make sure that provision is made for the use of suitable hardware components, such as operator channel extensions.

---

Automation systems are available in three different versions: standard, fault-tolerant, and fail-safe.

**Standard automation systems** consist of one or more S7-4xx CPUs.

**Fault-tolerant automation systems** consist of at least two redundant configured subsystems synchronized via fiber-optic cables. The user programs loaded in both CPUs are fully identical and are run synchronously by both CPUs. The failover has no effect on the active process, which continues uninterrupted.

The function of **fail-safe automation systems** in plants with high safety requirements is to detect errors/faults in the process, as well as internal errors/faults, and to automatically bring the plant to a safe state if an error/fault occurs. Relevant national regulations must be followed during development, commissioning, and operation of fail-safe systems.

S7 F systems provide a reference sum via the fail-safe program section. This sum is recorded and enables detection of changes in the fail-safe program.

### 3.1.2 Hardware Specification

The Hardware Design Specification (HDS) describes the architecture and configuration of the hardware. The HDS should define the points listed below, for example, which are later used as a test basis for the IQ and OQ.

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

The HDS can be formulated as part of the Functional Specification or in a separate document.



---

**Note**

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

---

---

**Note**

Information relating to the required content of an HDS can be found in **GAMP 4**, Annex D3.

---

### 3.1.3 Hardware Solutions for Special Automation Tasks

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

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

To keep validation work to a minimum, hardware components from the PCS 7 Add-On catalog should be given preference, where necessary.

## 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 linked to WEB clients, SIMATIC IT applications (MES interfaces), and customer-specific office networks and associated office applications are gaining in importance. The planning and configuration of networked PCS 7 automation solutions feature heavily when it comes to meeting these requirements and always ensuring the highest possible level of data security/integrity.

---

### Note

Siemens provides recommendations and information on planning and configuring networks in the manual ***PCS 7 Security concept PCS 7 and WinCC***.

---

### Ways of Improving Plant Security

PCS 7 offers several ways of improving information security within a plant. These include:

- Staggered user, group, and role concept
- SIMATIC Security Control (SSC)
- SCALANCE S firewall and VPN modules

For further information see chapter 4.6 Information Security.

### 3.3 Specification of Basic Software

The Software Design Specification (SDS) describes the architecture and configuration of the software. It includes a description of the application software, as well as a definition of the standard software components used in the system, which are specified by means of their designation, version number, etc. This description serves as a reference when performing subsequent tests (FAT, SAT, IQ, OQ).

Standard software components include automation software components and software provided by third parties.

- Operating system
- SIMATIC PCS 7 bundles, e.g. for OS server, OS client, CAS, engineering system, SIMATIC Logon, BATCH server, BATCH client, etc.
- Standard libraries (part of the engineering system)
- SIMATIC optional packages such as SIMATIC BATCH, SIMATIC Route Control, SIMATIC PDM, SFC Visualization, etc.); separate licenses are needed to use some of the optional packages.
- Acrobat Reader, MS Office (Word, Excel), etc.

#### 3.3.1 Operating System

All information relating to the operating system installation can be found in the current manual *PCS 7 PC-Configuration and Authorization*. Additional information on hardware and software requirements is also contained on the *SIMATIC PCS 7 Toolset-DVD* in the readme-file.

#### 3.3.2 Basic Software for User Administration

Access to the SIMATIC PCS 7 system components is controlled by SIMATIC Logon. Further information on the installation and configuration of the different SIMATIC Logon components can be found in chapter 4.3 as well as in the *Engineering Manual SIMATIC Logon*.

#### 3.3.3 Engineering System Software Components

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

#### Multiproject Engineering

See chapter 5.1 of this manual for information on how multiprojects are set up and used.



## **Process Control Libraries**

The process control libraries contain predefined and tested objects (blocks, faceplates, and symbols). When using these libraries, project engineering is generally restricted to the configuration of the corresponding objects. One major advantage of using predefined objects, when project engineering automated systems in the pharmaceutical industry, is the lower-level software categorization (see chapter 7.3.1) and the possibility of implementing updates. Also, less validation work than that involved with user-specific blocks is required.

## **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 chart, where they are interconnected and parameterized in accordance with requirements.

## **SFC (Sequential Function Chart)**

The SFC Editor facilitates the graphic configuration and commissioning of sequential controls. The most important components are steps and transitions, as well as parallel and alternative branches.

## **Import / Export Assistant**

The Import / Export Assistant (IEA) is a tool used to configure systems which feature recurring functions and/or plant units. Process tag lists or CAD charts already created in the planning phase are used during configuration to (largely automatically) create CFC charts for process tags. During this process, replicas of the models are generated and then supplied with specific data.

For further information on configuration and use of the IEA see chapter 6.2.

## **Version Trail**

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

For further information on configuration and use of "Version Trail" see chapter 7.4.1.

## **Version Cross Manager**

The Version Cross Manager (VXM) is an add-on package for PCS 7, which allows two PCS 7 user projects or libraries to be compared and any differences to be displayed. Multiprojects cannot be compared.

For further information on configuration and use of the VXM see chapter 7.4.2.

## Route Control

The SIMATIC Route Control optional 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 further information on configuration and use of "SIMATIC Route Control" see chapter 6.7.

## 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 PG/PC. The configured application software can then be tested without using AS hardware (CPU and/or signal modules). Only one CPU can be simulated at any one time. Communications processors and Route Control cannot be simulated.



---

### Notice

The use of S7 PLCSIM is of particular interest for the test system, for example, for typical tests. However, it should be noted that PLCSIM is linked via MPI. All connections must be reconfigured if they are to be subsequently used with an Ethernet network.

---

### 3.3.4 HMI Level Software Components

#### 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-user 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 created to increase availability.

Licenses for the operator stations are available in different sizes, depending on the size of the project and the number of process objects involved.



---

### Note

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

---

## OS Archiving

Process values and messages are stored in a short-term archive based on Microsoft SQL server technology. The data saved in the short-term archive can be stored in long-term archives, see chapter 6.12.2.

## SFC Visualization Additional Software

An SFC (sequential function chart) is used for the sequential control (also known as a sequencer) of processes. SFCs consist of a sequence of steps, which are separated from one another by the relevant step enabling conditions (known as transitions). 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 extra work is required to configure SFC Visualization.

## Open PCS 7 Additional Software

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 PCS 7 project topology being required. OPC (OLE for Process Control) refers to a uniform, vendor-independent software interface, whose standard was defined by the OPC Foundation. The OPC Foundation is an alliance of leading companies in the field of industrial automation. Information on OPC can be found on the Internet at <http://www.opcfoundation.org>; the use of "Open PCS 7" is described in more detail in chapter 6.5.2.

## OS Web Client Additional Software

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

---

### Note

Use of the Web Option in a controlled environment must be thoroughly discussed with the customer. Issues such as access to the Web client, critical or non-critical operator control and monitoring functions, logon, and audit trail, as well as a secure data connection, must be considered during these discussions.

---

For further information on the use and the configuration of PCS 7 OS Web Option refer to chapter 6.5.1 as well as manual **PCS 7 OS Web Option**.

### 3.3.5 SIMATIC BATCH Basics and Options

The SIMATIC BATCH software is integrated in SIMATIC PCS 7. 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.

Basic SIMATIC BATCH components include the “Batch Control Center” (BatchCC), used for the operator control and monitoring of the recipe control strategy, and the “Recipe Editor” (recipe system), used for creating and managing master recipes and library operations.

Several useful optional packages are available in addition to the basic configuration:

- **ROP Library**  
Managing recipe operations from a central location ensures that changes can be made centrally and that any such changes are passed on to all instances. The reference to the master module can be resolved at a later point in the project.
- **Hierarchical Recipe**  
Recipe procedures, recipe unit procedures, and recipe operations for performing the process engineering task can be clearly structured.
- **Separation Procedures / Formulas**  
Separating the procedure and the parameter sets further increases flexibility by means of recipes which are not specific to a particular unit.
- **SIMATIC BATCH API**  
The SIMATIC BATCH application programming interface (API) is an open interface, which enables the user to access SIMATIC BATCH data and functions via the plant control level, for example.
- **Batch Planning**  
Batch planning and control are supported in a user-friendly manner and simplified, thanks to special displays such as the order category list, production order list, batch planning list, batch status list, or batch results list.

Refer to the system documentation for more information on using and configuring the optional packages.

## **3.4 SIMATIC Additional Software**

### **3.4.1 SIMATIC PCS 7 Add-Ons**

The SIMATIC PCS 7 Add-On catalog contains solutions for various areas of application or special industries, such as the process industries. For the listed add-ons the catalog also contains addresses for the responsible people you will need to contact.

---

#### **Note**

For the realization of functions not covered by standard PCS 7, you should preferentially use the add-ons from the current catalogues.

[https://pcs.khe.siemens.com/index\\_pcs\\_7\\_add\\_ons-6815.htm](https://pcs.khe.siemens.com/index_pcs_7_add_ons-6815.htm)

---

### **3.4.2 Long-Term Archiving with StoragePlus**

StoragePlus (see also chapter 6.12.4) is used for the long-term archiving of process values, messages, batch data, and reports from up to four servers. The archives managed using StoragePlus can be cataloged and transferred to an external medium. Items of process-value data can be accepted at a maximum rate of 1,000 per second per server; if data is accepted from more than one server at once, the maximum rate is 1,600 per second.

### **3.4.3 Long-Term Archiving with the Central Archive Server (CAS)**

The central archive server (CAS) is used for the long-term archiving of process values, messages, batch data, and reports from up to 11 servers; see also chapter 6.12.3. The archives managed using the CAS (process values, messages, batch data) can be cataloged and transferred to an external medium. Items of process-value data can be accepted at a maximum rate of 1,000 per second per server; if data is accepted from more than one server at once, the maximum rate is 10,000 per second.

The CAS server can also have a redundant design if required.

### 3.5 Application Software Specifications

As well as defining the standard software components used, another essential task of the Software Design Specification (SDS) is to specify the application software. This is then used as a basis for subsequent testing of the application software (FAT, SAT, IQ, OQ).

The SDS can be integrated in other specification documents (FS, DS). However, part of this specification usually takes the form of other, separate documents, such as a process tag list, I/O list, parameter list, P&I, etc. The status of these documents (version, release) must be well defined, as it must for other specification documents (URS, FS, DS).

The SDS includes the following, for example:

- Plant hierarchy
- Software structure
- Archiving, messages, trends, etc.
- Module specification, possibly in a separate document,

provided that these have not already been sufficiently defined in the FS.

---

#### Note

There are standards governing the description of software structures, such as *ANSI/ISA-88.01*.

SIMATIC PCS 7 uses the model of the *ANSI/ISA-88.01* as a basis for configuring batch control, see also chapter 6.6.3.

---

---

#### Note

Additional information relating to the required content of software specifications can be found in **GAMP 4**, Annex D4.

---

## 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, there can be no guarantee that the system will operate without any problems.

### 3.6.2 Virus Scanners

The use of virus scanners during process mode (runtime) is permitted. More information on selecting, configuring, and updating virus scanners can be found in the PCS 7 readme files and in FAQ 10154608 as well as the manual **PCS 7 Setting up antivirus software**.

If 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 only check incoming data traffic.
- The time-controlled search must be deactivated, as it significantly limits system performance in process mode.
- A manual search must not be executed in process mode. It can be performed at regular intervals, e.g. during maintenance cycles.

Specifications like these should be laid down in an SOP.

### 3.6.3 Image & Partition Tools

Commercially available additional software concerning “Image” and “Partition” allows users to make data backups of hard disk content. Backing up system and application software means that the system can be restored quickly. Backed-up contents of hard disks can also be copied back to devices with an identical configuration. This simplifies the procedure for replacing computers.

Apart from creating hard disk images, many of these software programs can also be used to create, modify, and delete hard disk partitions.

---

#### Note

The created images are used to restore the installed system, but not to back up online data.

For the selection and configuration of those software components the user needs to have system administration knowledge.

---

## 4 System Installation

### 4.1 Installing the Operating System

When selecting the operating system, observe the information given in chapter 3 and the sources named therein.

The operating system must be installed in accordance with the *Installation Guidelines for Operating System*.

The manual **PCS 7 PC-Configuration and Authorization** also contains information on installing PC stations.

### 4.2 Installing PCS 7

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

- Manual **PCS 7 Security concept PCS 7 and WinCC**
- Manual **PCS 7 PC-Configuration and Authorization**
- Manual **PCS 7 Released Modules**
- PCS 7 **Installation DVD, Readme**

---

#### Note

SIMATIC Logon must be selected in the installation setup.

---



## 4.3 Setting Up User Administration

An automated system is safeguarded against unauthorized access by activating access protection, which protects against access on the input level and the ES and OS configuration level, as well as to backup copies and archives. Also, one of the most important basic features for meeting pharmaceutical requirements is that operator actions can only be performed subject to a user-specific logon/logoff procedure.

### 4.3.1 User Administration on the Operating System Level

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

- In a domain
- In a workgroup



---

#### Note

The full name of every user must be entered in "Local Users and Groups" in Windows Computer Management. This name is used by the application for display in SIMATIC PCS 7 following logon. Therefore, this field must not be left blank!

---

For further information see manual **PCS 7 Security concept PCS 7 and WinCC**.

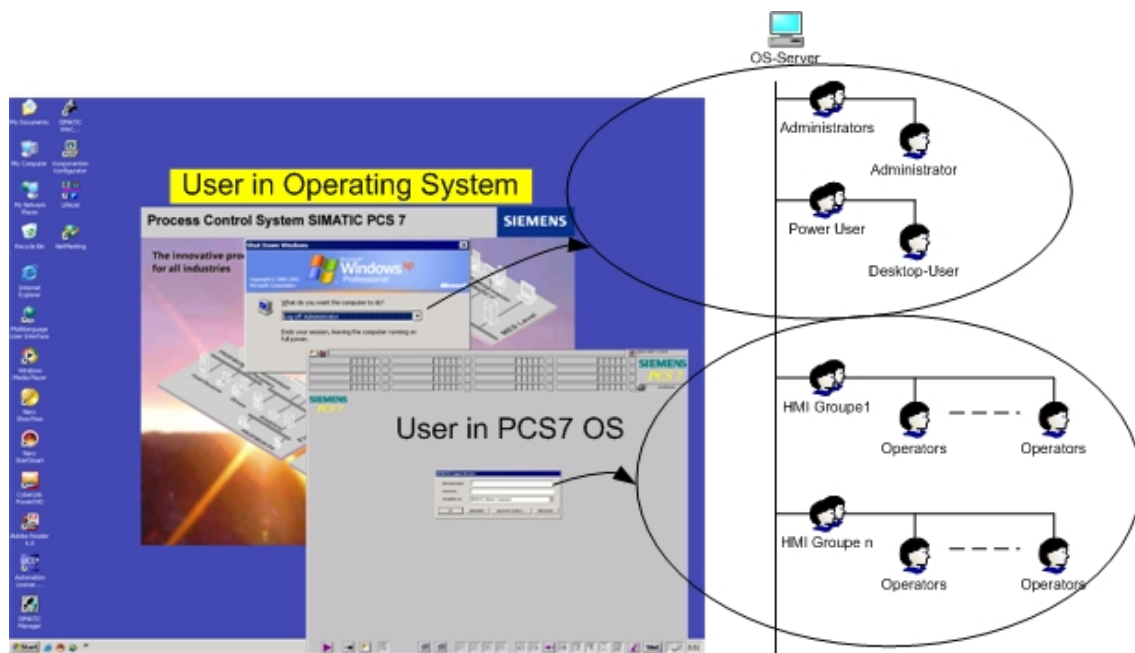
When a user logs on to the SIMATIC environment, his operator rights are authenticated; however, a "standard user", who possesses the rights required for the operating system level ("power user" as a minimum), is always logged on to the operating system at the same time.

---

#### Note

The user logged on to the operating system should be the same one throughout the entire system; he should be logged on automatically when an OS computer powers up.

---

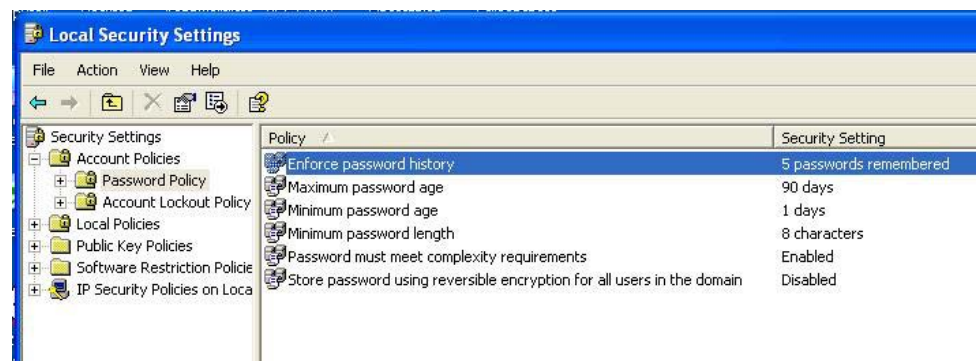


#### Note

Logon and logoff activities as well as unsuccessful logon attempts can be viewed and exported via the SIMATIC Logon Eventlog Viewer.

Changes to the user and group configuration are recorded on the operating system level.

### 4.3.2 Security Settings



#### Note

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

## Password Policy

The password policy security settings are made in the operating system.

Guideline	Description of the security setting
Enforce password history	Specifies the number of unique new passwords that must be used for a user account before an old password can be used again.
Password must meet complexity requirements	When activated, the password must be made up of at least three of the four following categories: <ol style="list-style-type: none"><li>1. A-Z uppercase letters</li><li>2. a-z lowercase letters</li><li>3. 0-9 numeric characters</li><li>4. !,\$,%, etc. special characters</li></ol>
Maximum password length	Specifies the minimum number of characters a password must contain.
Maximum password age	Specifies the maximum time that a password may be used before it must be changed.
Minimum password age	Specifies the minimum time that a password must be used.

Recommendations on how to choose good, secure passwords can be found in several publications.

## Account Lockout Policies

The security mechanisms for account lockout policies, such as the number of permissible failed logon attempts, are set in the operating system.

Guideline	Description of the security setting
Account lockout threshold	Specifies the number of failed attempted logons before the user account is locked out.
Account lockout duration	Specifies how long an account remains locked out before the lockout is canceled automatically. If the value 0 is set, the account remains locked out until it is unlocked by an administrator. This is the recommended setting.
Reset account lockout counter after	Specifies how many minutes it takes after failed logon attempts before the account lockout counter is reset.

## Audit Policies

The security mechanisms for audit policies relating to logon attempts, account management activities, etc. are set in the operating system.

Guideline	Description of the security setting
Audit logon attempts	Specifies whether or not the instance of a user logging on to a computer is audited.
Audit account management	Specifies whether or not the individual events of account management are audited (creating or changing a user account, changing or setting passwords).
Audit logon events	Specifies whether or not each instance of a user logging on to or off from a computer is audited.
Audit policy change	Specifies whether or not every incidence of a change to user rights assignment policies, audit policies, or trust policies is audited.

### Note

In order to enable logon activities to be traced at a later date, the required settings must be made in the audit policy of the local policies of Windows, but also those in SIMATIC Logon according to chapter 4.3.4.

### 4.3.3 Managing SIMATIC User Groups

When PCS 7 is installed, default SIMATIC user groups are created in the operating system automatically (SIMATIC HMI, etc.). These must not be changed or deleted. The manual **PCS 7 Security concept PCS 7 and WinCC**, chapter 3, contains additional information on the created groups.

### Note

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



### Note

If multiple servers or redundant servers are used, the Windows domain concept must be used for user administration. The use of two domain servers ensures that users will still be able to perform operations and/or log on even if one domain server fails. The domain servers must be installed on separate computers; it is not permitted to install the domain server functionality on a PCS 7 system.

#### 4.3.4 Configuring SIMATIC Logon

The basic settings for configuring SIMATIC Logon are made with the "Configure SIMATIC Logon" dialog. The available settings are described in the *Engineering Manual SIMATIC Logon*.

---

**Note**

Events such as successful and failed logon/logoff activities, password changes, etc. are stored in the SIMATIC Logon EventLog database. This must be taken into account when backing up data.

---

#### Automatic Logoff

To prevent somebody to misuse the logged-on user name for unauthorized system access, the "Automatic Logoff" function must be activated in the SIMATIC Logon configuration for a set period of time.



---

**Note**

The "Automatic Logoff" function must be deactivated on the operating system level, otherwise the user interface will close down completely.

Furthermore the activation of a screensaver in conjunction with SIMATIC Logon is not permitted.

---

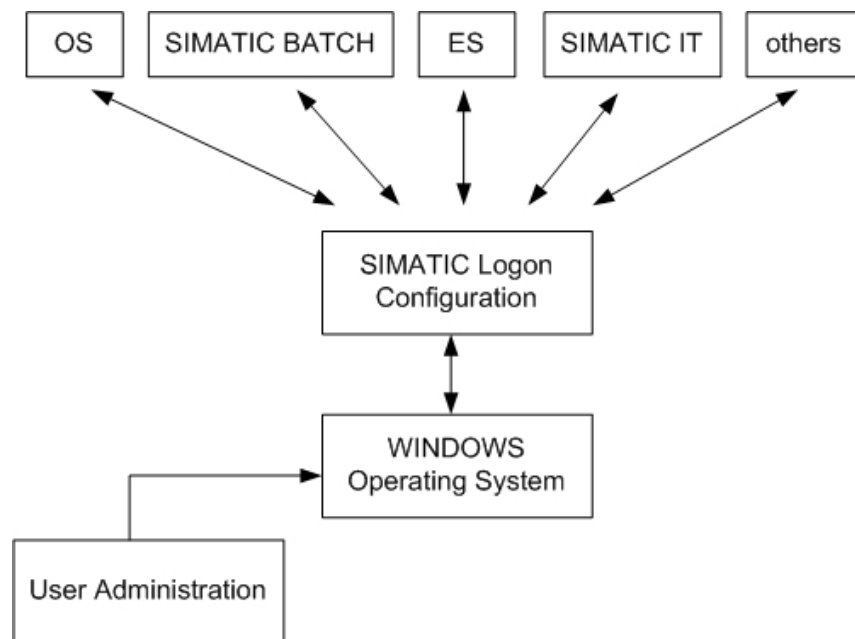
#### Default User after User Logs Off

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

In contrast to all other users, the "default user" does not need to be created as a Windows user. The "default user" is a member of the "DefaultGroup" and "Emergency\_Operator" roles. The rights for these groups are specified in the relevant PCS 7 OS (server/client) applications.

### 4.3.5 Access Protection

The SIMATIC Logon Service must be installed in order for access protection to be activated. SIMATIC Logon maintains users and user groups by means of the operating system's user administration. The rights of the various users (user groups) as regards operator actions and the way in which these are logged in the system are assigned on the input level in SIMATIC OS and SIMATIC BATCH and on the engineering level in SIMATIC ES, in accordance with the system specification.



The following order must be adhered to:

- Setup of user groups and users under Windows
- Configuration of SIMATIC Logon
- Creation of a project
- Administration of user rights for the individual SIMATIC components (ES, OS, BATCH)



#### Note

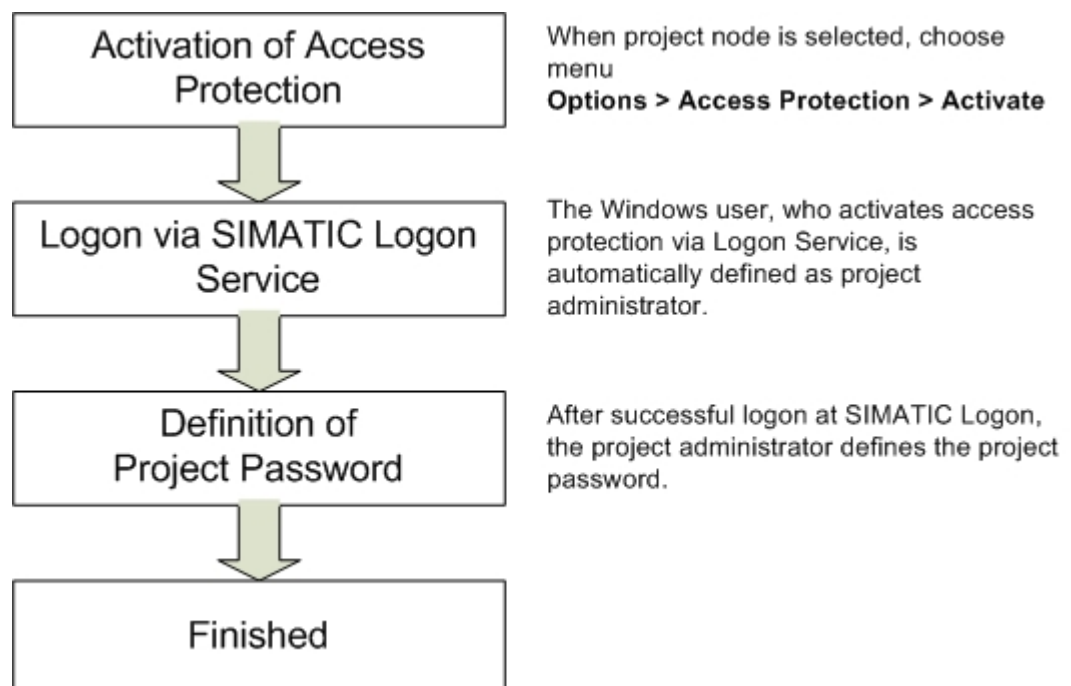
Access protection must have been set up in full prior to starting configuration and must also be integrated in the typical description.

All permission levels of the visualization interface (faceplates, entry fields, buttons, etc.) must be set up in accordance with specifications (URS, FS, DS) and tested during the course of the project.

## 4.4 Administration of User Rights

### 4.4.1 Rights Management on the ES

Access to projects and libraries can be controlled using SIMATIC Logon. When activating access protection 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 be known to the project administrators only.



"SIMATIC Logon Role Management" serves as the interface for assigning users to the groups 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.

The time at which access protection is to be activated on the ES level should be specified at an early stage of the project.

---

The two types of user rights on the ES level are:

### **Project Editor**

- Making project changes
- Displaying the change log

### **Project Administrator**

- Making project changes
- Displaying the change log
- Activating and deactivating the change log
- Managing access protection
- Deactivating access protection
- Synchronizing access protection in the multiproject



---

**Note**

The project format is changed when access protection is activated for the first time. From that point, the project can no longer be edited using a STEP 7 version < V5.4.

---

The following information relates to the individual phases/scenarios which arise when setting up and using protected projects/libraries:

### **Managing Users**

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

#### **Scenario 1**

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

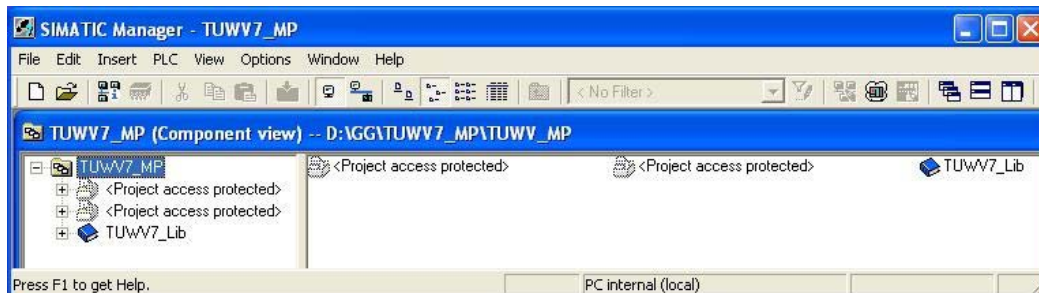
As long as the user has the required permission, he can open a project without any further authentication, provided that it is in the same network as the user. This also applies if the project has been taken out of the multiproject.

#### **Scenario 2**

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



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



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



---

### Note

Only project administrators should have knowledge of the project password.

---

## 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. It is also the case here that 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.

---

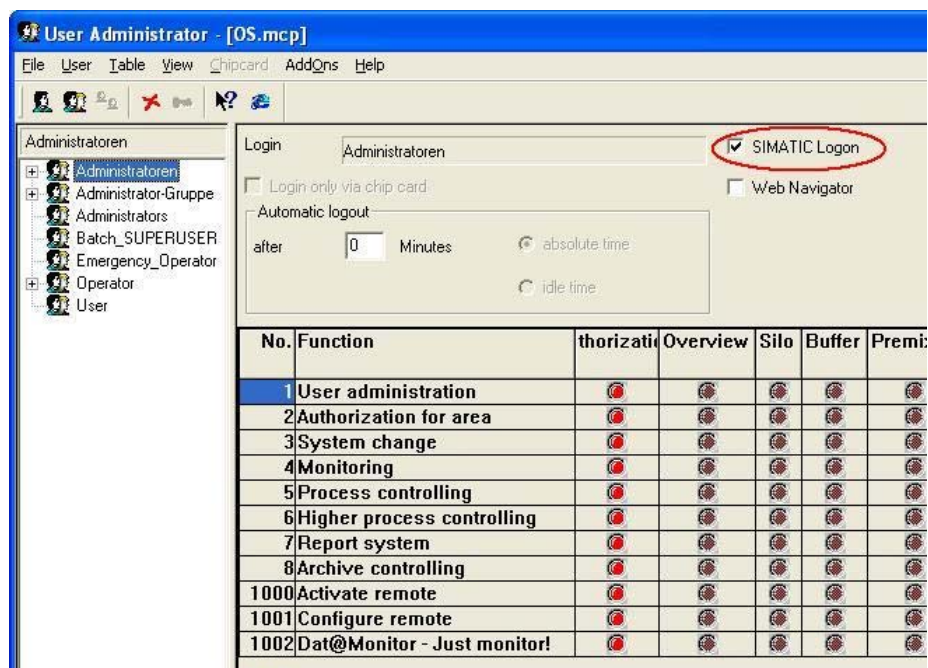
For further information refer to manual **PCS 7 V7.0 SP1 Engineering System**.

#### 4.4.2 Rights Management on the OS

Windows groups are assigned to PCS 7 OS groups by creating groups of the same name. If you want to assign a Windows group named “Operator”, for example, a group also called “Operator” must be created in the PCS 7 OS User Administrator and the required rights assigned. The following procedure must be adhered to:

- Open PCS 7 OS project.
- Open User Administrator using WinCC Control Center.
- Create the group(s).
- Assign rights to each group.

The figure below shows how operator rights are assigned to individual groups.

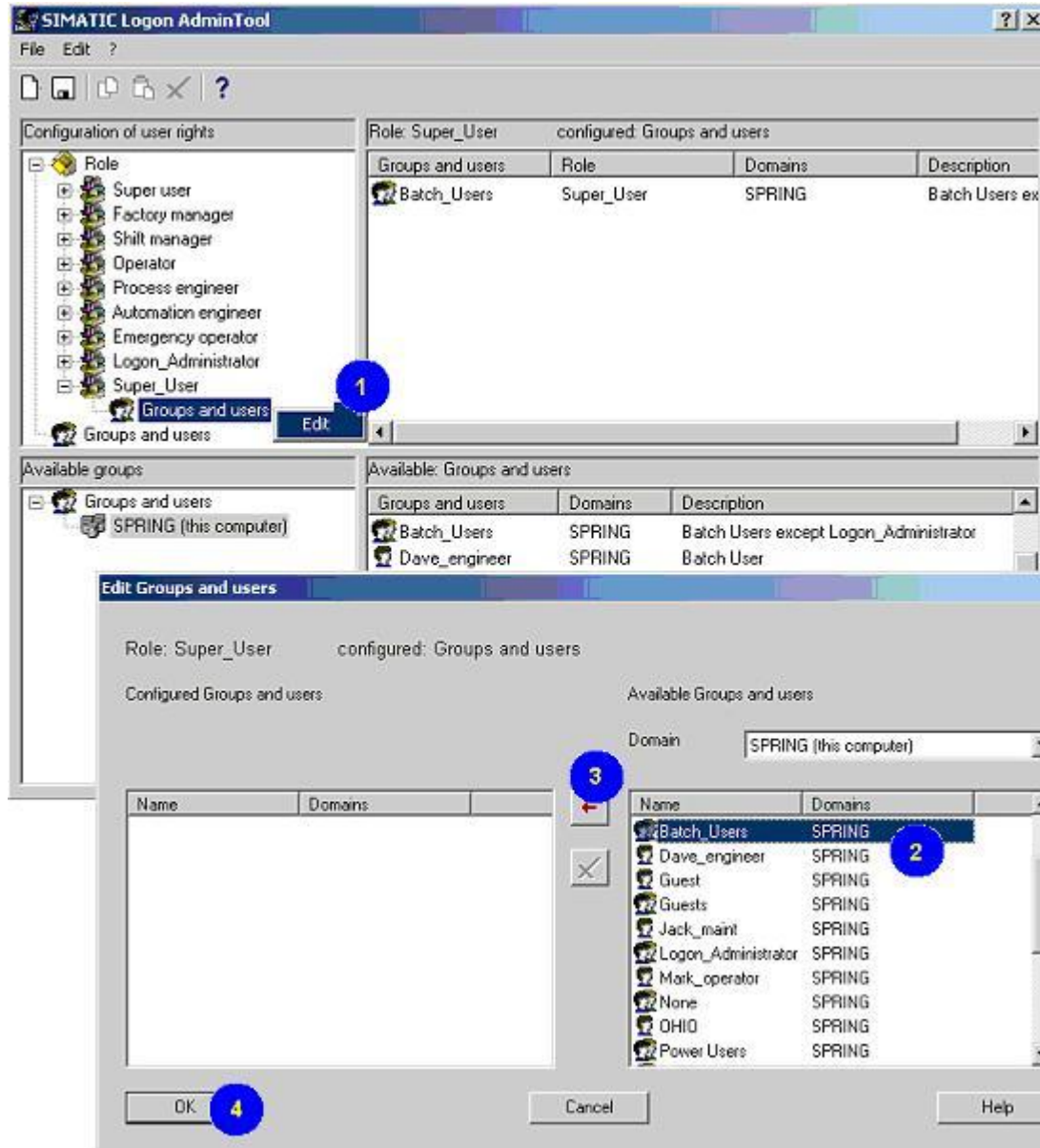


#### Note

The check mark for activating SIMATIC Logon must be set in the PCS 7 OS “User Administration” of the relevant PCS 7 OS computer.

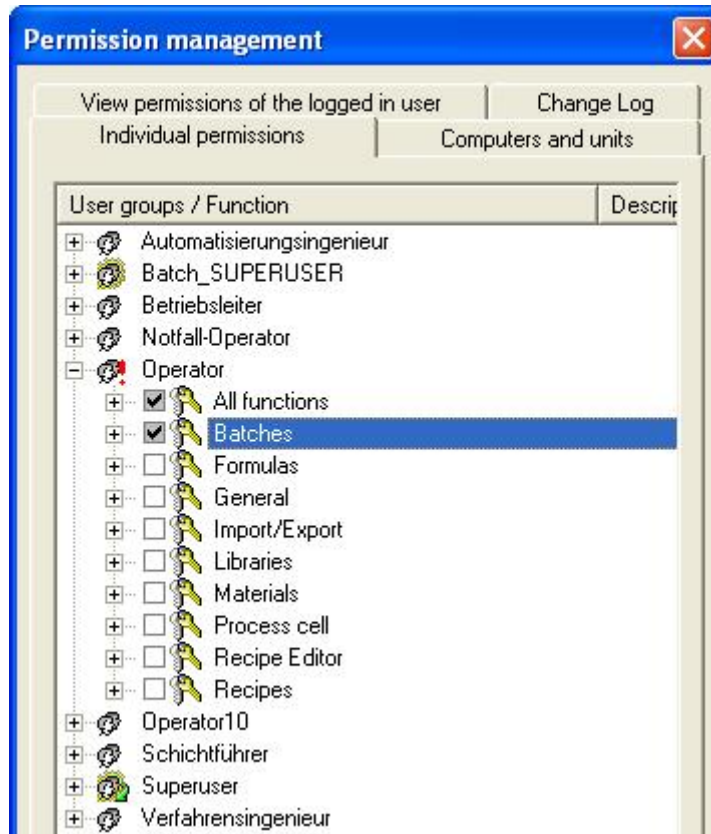
#### 4.4.3 Rights Management in SIMATIC BATCH

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



The individual roles are assigned to operator rights in SIMATIC BATCH. In addition, the following can also be defined:

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



## 4.5 Configuring Access Protection

See manuals **PCS 7 Engineering System** and **PCS 7 Security concept PCS 7 and WinCC** for information on the general network configuration.

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 solely for administrators or technical maintenance personnel.

---

### Automatic Power Up and Logon

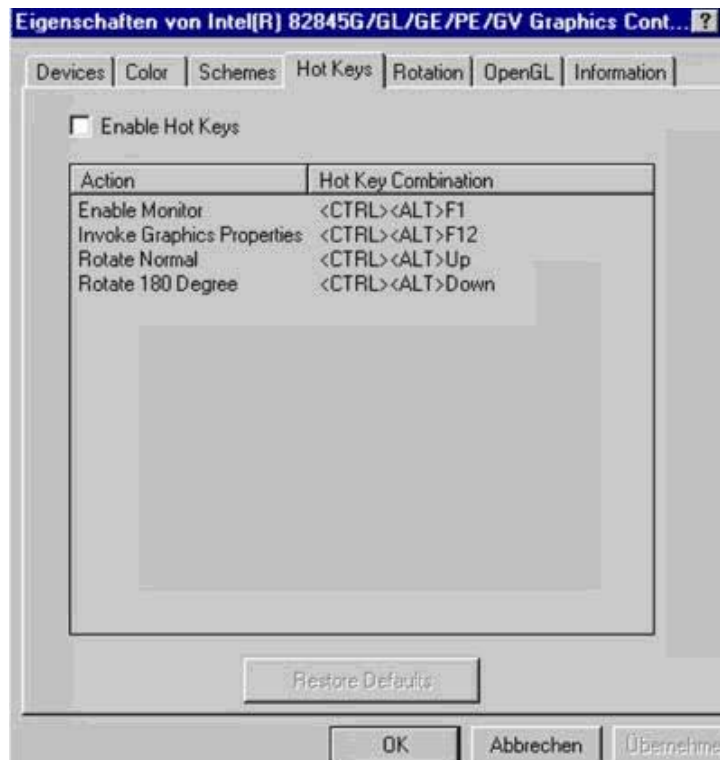
The “default user” on the operating system level must be logged on automatically when each server or client is started up.

### Activating the Input Level (Runtime)

Automatic starting of the PCS 7 input level (runtime) must be activated so that the operating system level cannot be accessed.

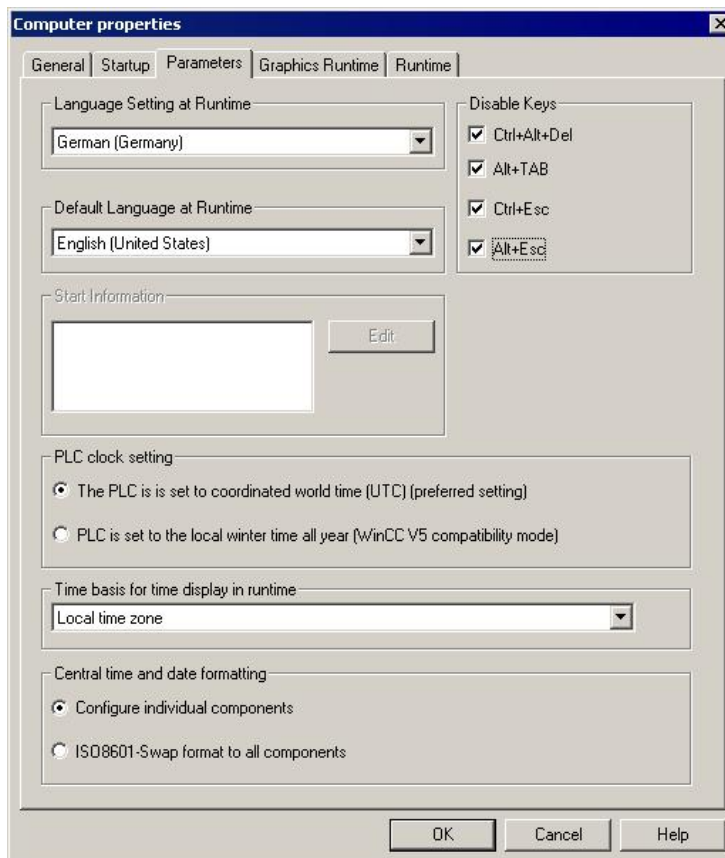
### 4.5.1 Configuration Settings in Windows

Using hot keys to adjust graphics card settings allows you to go to the operating system user interface. Therefore, this option must be deactivated for operator stations in particular.



## 4.5.2 Configuration Settings on SIMATIC PCS 7 OS

Access to the operating system during process operation (runtime) is configured via the OS parameter properties. The necessary settings are shown in the figure below.




---

### Note

It must also be ensured in PCS 7 OS user administration that the button for exiting 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

### 4.6.1 SIMATIC Security Control (SSC)

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

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

Following installation, the Start > SIMATIC > SimaticSecurityControl menu command can be used to execute the 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 a different working environment (domain or workgroup), it must be reconfigured.

---

### 4.6.2 SCALANCE S

The increasing integration of plant networks into office networks brings with it a rise in associated security risks, from network problems such as the duplicate assignment of network addresses, to problems with viruses, and even the possibility of attacks by computer hackers.

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.

For details see FAQ to topic “firewall” (in the area “Communication/Networks”), as well as document 22376747 “Protection of an Automation Cell Using Firewall” and its appended document.



## **VPN**

A virtual private network links external computers to the local network and is also able to encrypt the transferred data. A VPN connection enables external systems to perform secure remote access over the Internet. To do this, SCALANCE S technology uses the IPSec protocol, which provides an extremely high level of security in tunnel mode (VPN tunnel).

For details see FAQ to topic "VPN tunnel" (in the area "Communication/Networks") as well as document 22056713 "Security via VPN Tunnels secured by IPSec" and its appended document.

---

### **Note**

SCALANCE S technology offers various applications. More information can be found in the SCALANCE manuals.

---

## 5 Project Settings and Definitions

### 5.1 Multiproject Setup

Multiproject engineering allows a project to be divided into several subprojects 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.

---

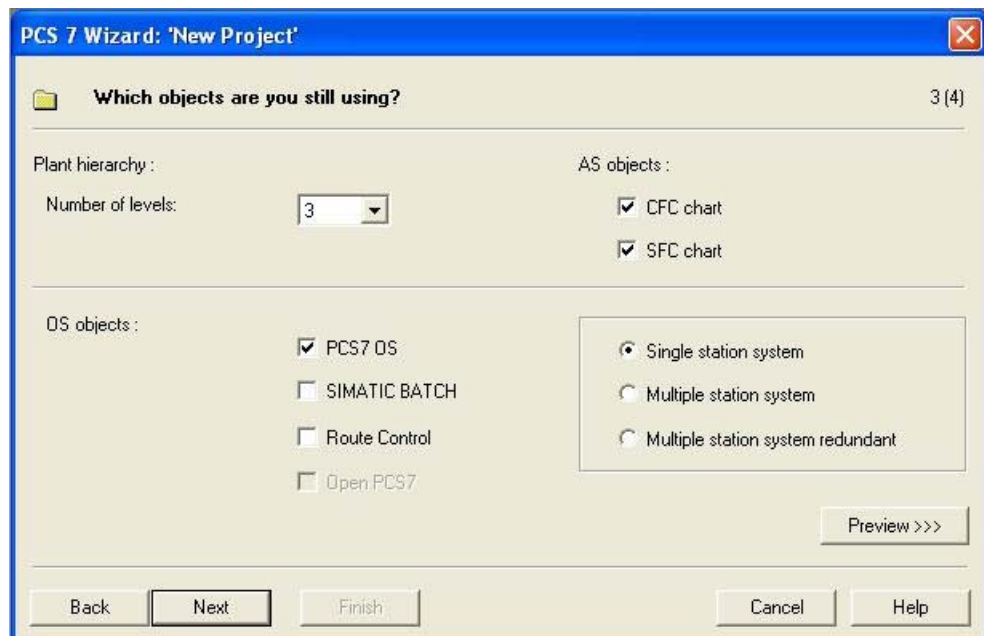
#### Note

In a controlled environment in particular, it is essential to use the master data library to centrally manage process tag types, models, SFC types, and shared declarations.

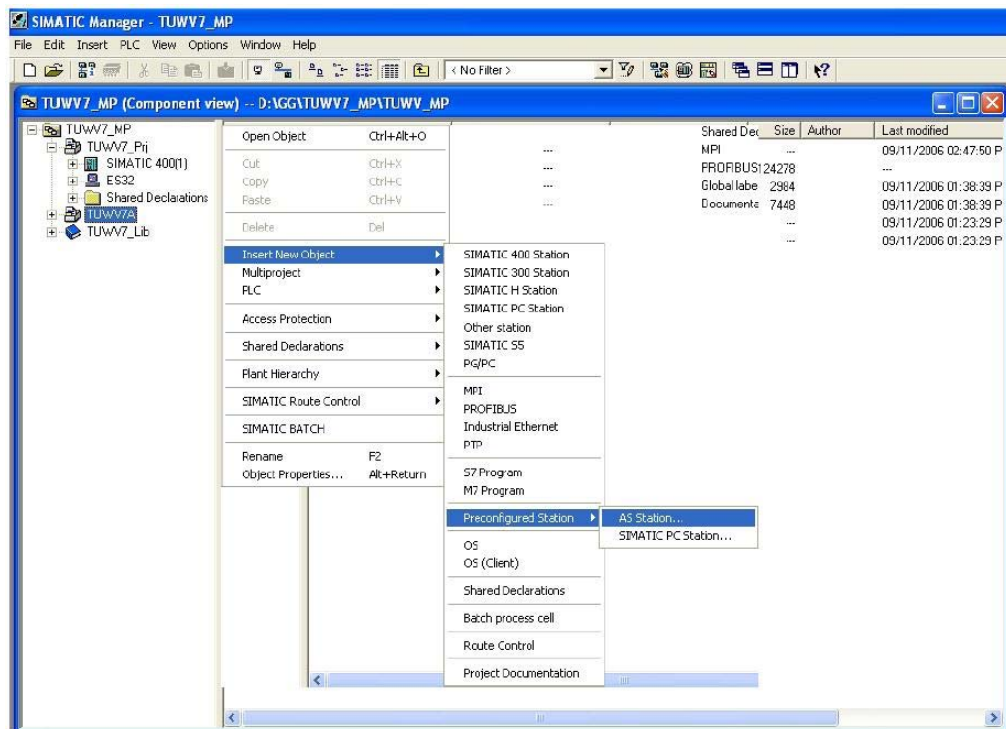
---

The “New Project” SIMATIC PCS 7 Wizard supports you when you create projects. In using it, a multiproject is created automatically. The project name to be assigned should have been previously defined in the software specification, as it can be difficult to subsequently rename a project.

The OS objects are selected in a dialog box before a multiproject is made available, together with a project and the master data library.



A new project can be added to an existing multiproject as an empty or a preconfigured project:



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 only too happy to assist you with this.

## 5.2 Referenced OS Stations

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

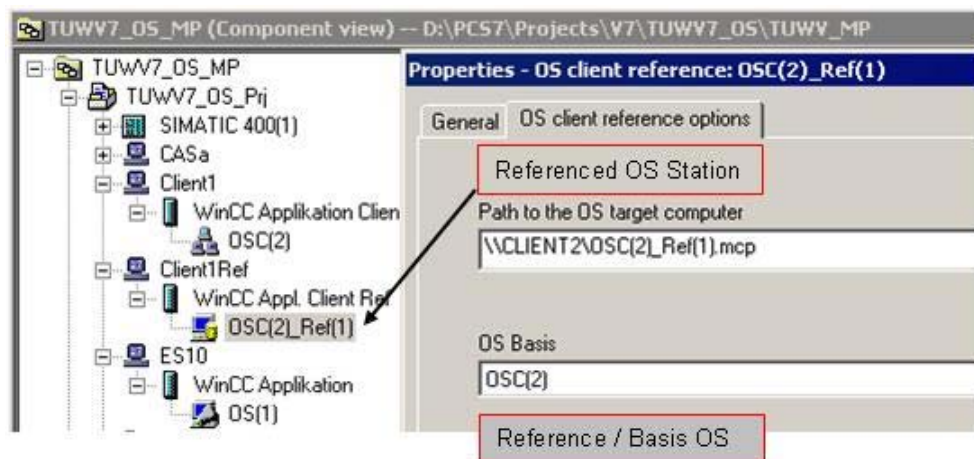
### Configuration Types

A reference can be created to one of the two types of OS station below:

- 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 “basic OS” is defined in the object properties (see figure). The possible number of referenced OS client stations is limited by the maximum number of operator stations, which is defined by PCS 7.



#### Note

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

### Advantages of Using Referenced Stations

Referenced stations help to minimize errors and the amount of work required. Only the reference station has to be tested thoroughly in accordance with its specification. All that needs to be done in terms of the referenced stations is to take special configuration features, such as screen resolutions, PCS 7 client-specific operating ranges, or user rights into account and to perform general function tests.

## 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 process tag types and models, but also the folders for shared declarations (units, enumerations, and equipment properties).

The project typicals are created on the basis of the libraries used (PCS 7 standard library, PTE-400, etc.); they are then stored and managed in the master data library.

---

### Note

The modules and typicals must be verified by means of a module test and approved by the customer prior to instantiation.

---

Not only must the same versions of blocks, SFC types, and typicals be used in all projects within a multiproject, but such projects must also be based on the same plant hierarchy and shared declarations. The individual projects are synchronized with the master data library to this end. The FAQ pages in the Intranet and the two documents 22258951 and 23785345 about Multiproject Engineering (see Service&Support pages – “Applications & Tools”) contain more helpful information.

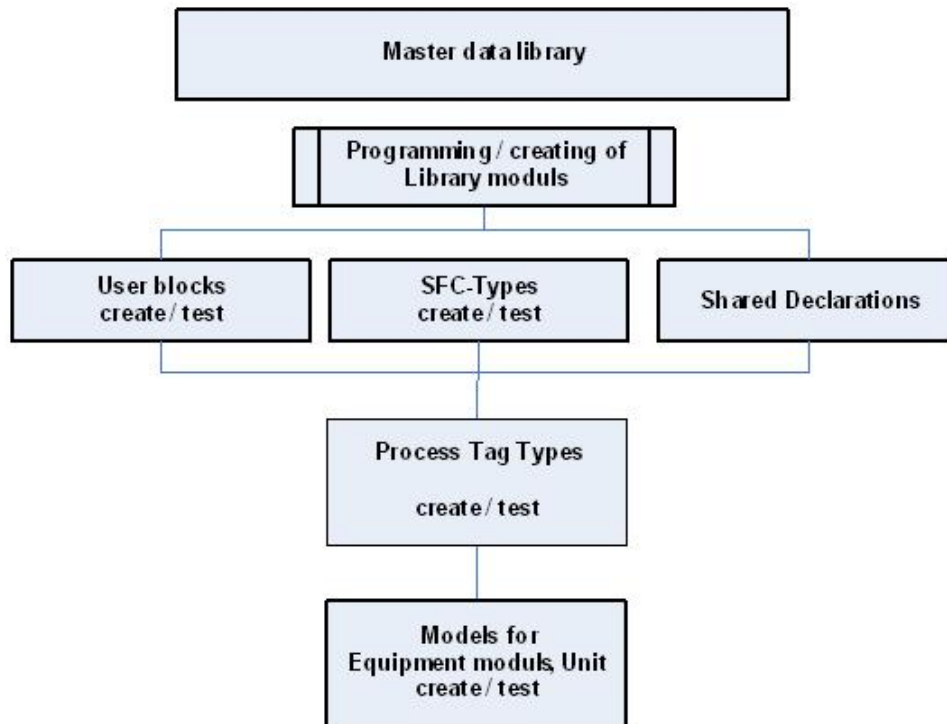
---

### Note

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

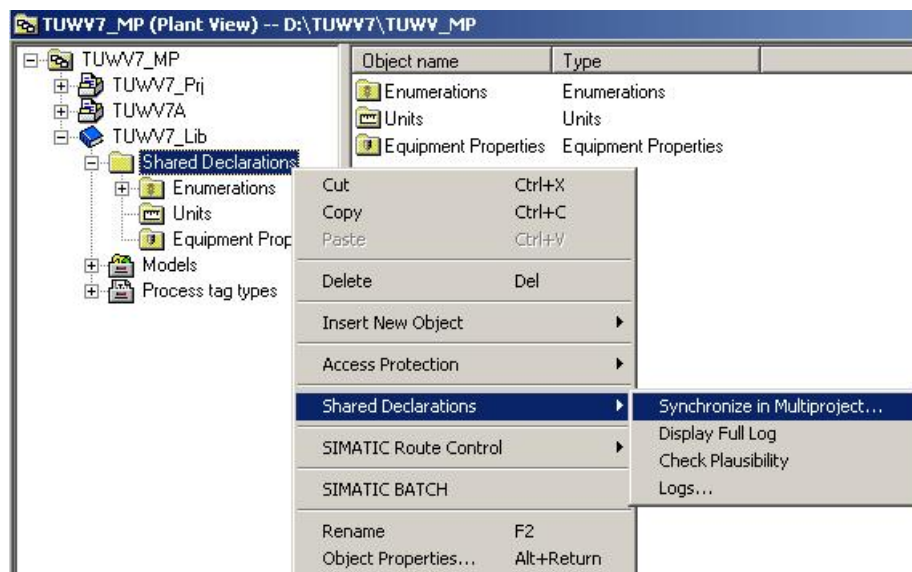
---

The function blocks, SFC types, and shared declarations are the smallest application software modules. These are used in creating process tag types and models, which are then duplicated either manually or via the IEA interface, see also chapter 6.2.



### 5.3.1 Synchronizing Shared Declarations

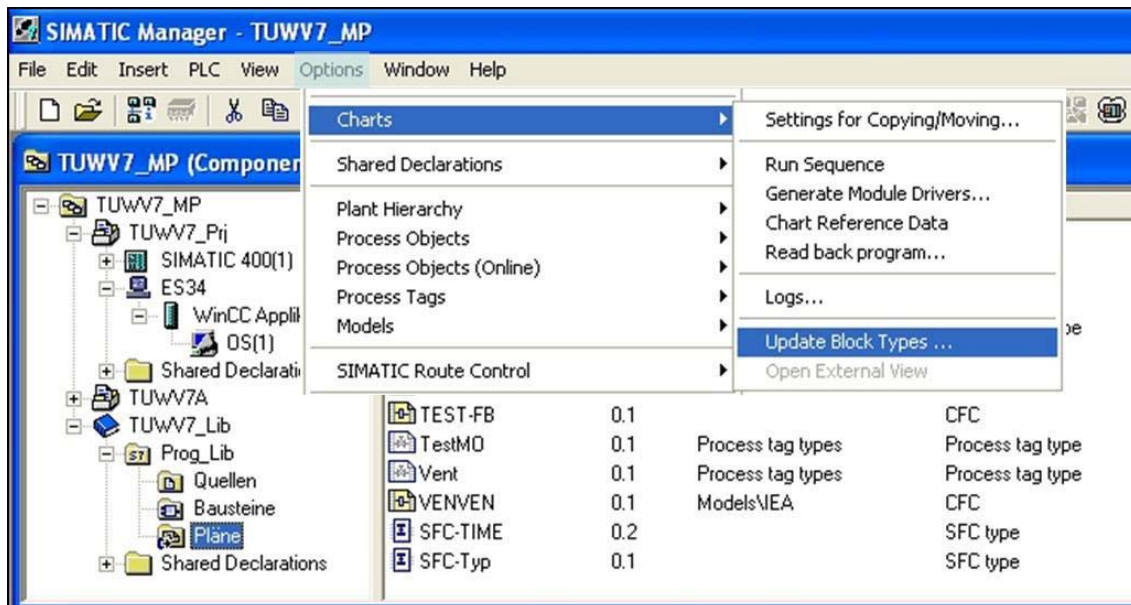
Shared declarations are generated in the master data library automatically when the multiproject is created. These declarations can be synchronized to make them available in all projects. Central maintenance in the master data library is strongly recommended in order to ensure consistency throughout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



### 5.3.2 Synchronizing SFC Types

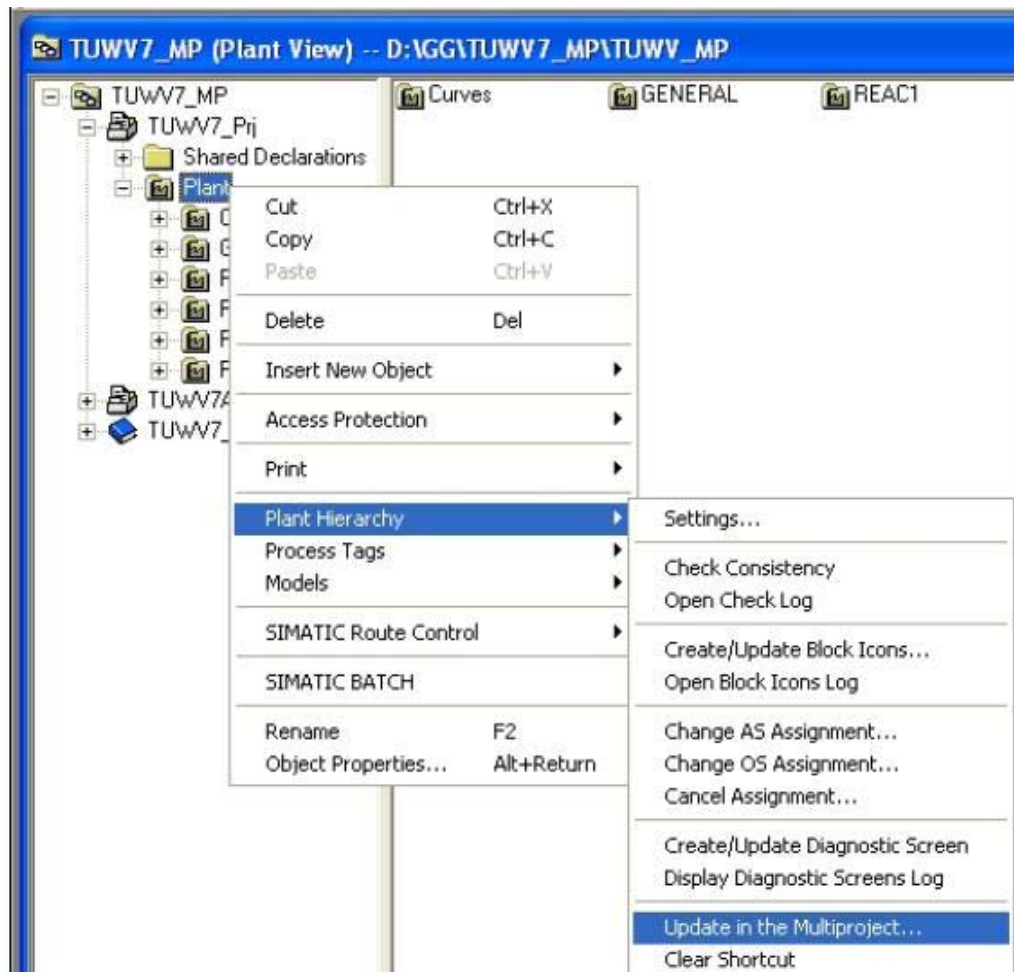
SFC types must be created and maintained in the master data library in order to achieve data consistency. These types can be synchronized to make the current SFC types available in the projects.

Deviations can be evaluated using the Version Cross Manager prior to synchronization.



### 5.3.3 Synchronizing the Plant Hierarchy

It is advisable to structure the plant hierarchy (PH) in the same way in all projects within a multiproject. To this end, the PH is created in one project (preferably the OS project) and the structure is then transferred to all other projects within the multiproject. The shared declarations of the sample project are also transferred to the selected projects as part of this process. This forms a connection between the hierarchy folders.



#### Note

The sample project takes on a kind of master role, i.e. 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 canceled.



## 5.4 Views

Three 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 centrally editing parameters, signals, messages, picture objects, archive tags, etc.

## 5.5 SIMATIC NET

### 5.5.1 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. Compliance with this requirement is subsequently checked within the framework of the IQ.

The gateways are configured using the “Advanced PC Configuration” tool. 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.

More information can be found in the **SIMATIC NET** documentation.

## 5.5.2 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 the plant bus and the terminal bus. To guarantee a high degree of security and performance, it is advisable to install these two buses separately.

### Industrial Ethernet Plant Bus

Industrial Ethernet is used as the plant bus. Industrial Ethernet uses the CSMA/CD (carrier sense multiple access with collision detection) access method standardized in IEEE 802.3.

The automation stations are connected with the OS servers and the engineering station via the plant bus. The ISO protocol is generally used as the transport protocol.

### Ethernet Terminal Bus

The PCS 7 servers are connected with the clients, archive servers, and higher-level MES systems via the terminal bus. The TCP/IP protocol is normally used as the transport protocol.

## 5.5.3 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 powerful real-time bus system such as PROFIBUS versions DP and PA. For more information, refer to manual **SIMATIC NET PROFIBUS Networks**.

---

### 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 application software. This has corresponding advantages in terms of regular data backups and verification of the software within the framework of the IQ/OQ.

---

## 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 even be used in hazardous zone 1. This makes data transfer rates of up to 1.5 Mbit/s 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 zone 0/1)

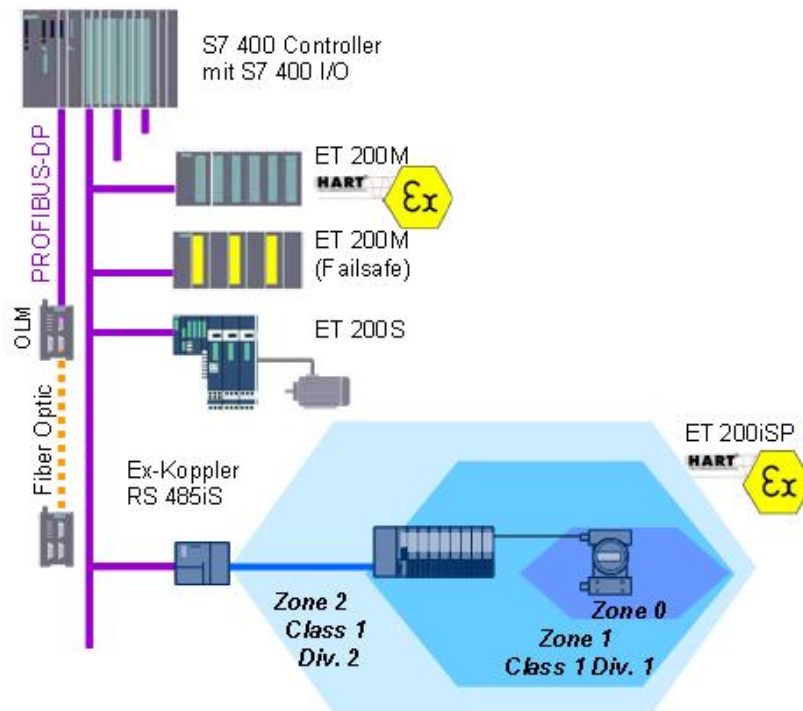
HART modules can be configured via the PDM, see chapter 5.5.4.

### PROFIBUS DP configuration

PROFIBUS DP is configured in HW Config. Components are selected from the hardware catalog by means of their order numbers, connected using drag & drop, and configured. Hardware not contained in the catalog can be installed in the SIMATIC PCS 7 hardware catalog via GSD files (device-specific device master data files). The newly installed devices are then available for configuration.

PROFIBUS DP single-channel configuration

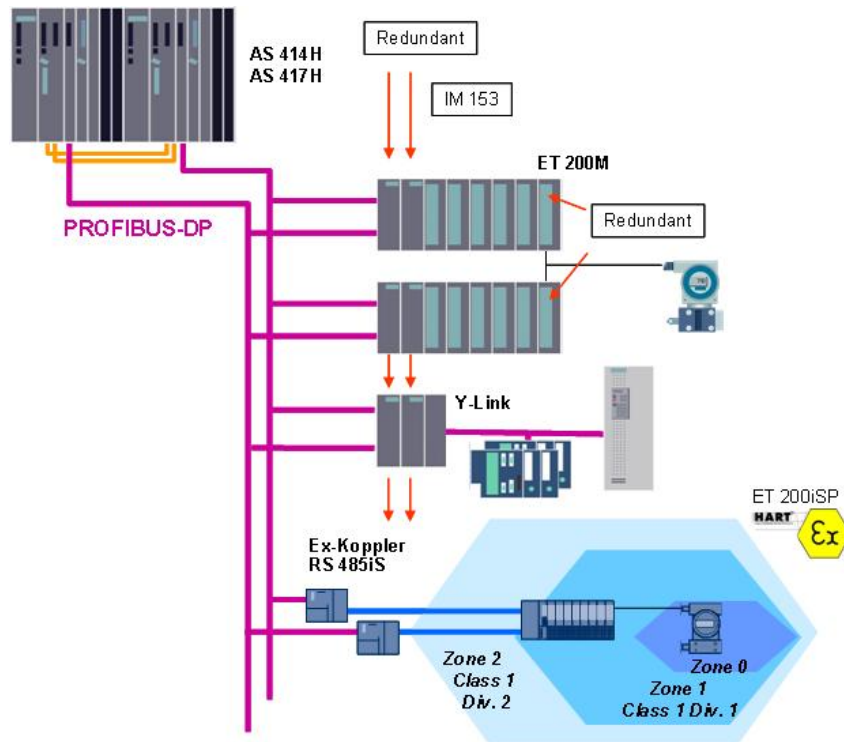
Different I/O module types can be used for different applications, as shown below.



### PROFIBUS DP redundant configuration

Distributed I/O devices such as ET 200M or ET 200iSP are available for redundant operation. The stations are connected to a fault-tolerant AS over two redundant PROFIBUS DP lines.

There is also the option to connect non-redundant PROFIBUS DP devices over a Y link.

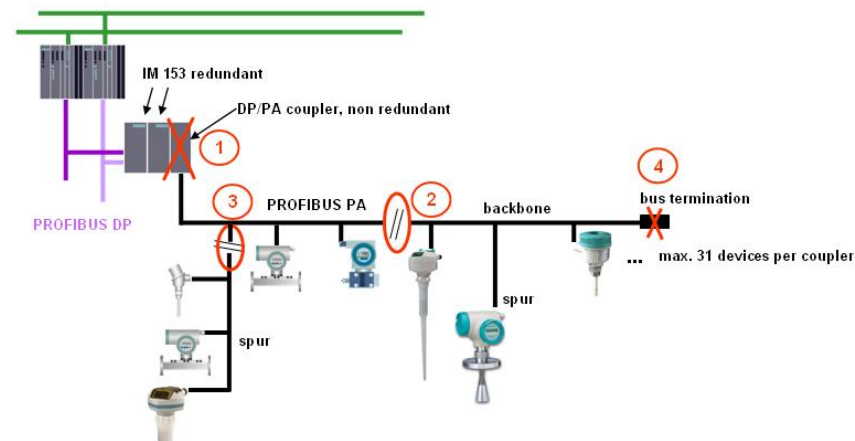


## PROFIBUS PA

### PROFIBUS PA simple configuration

For information on non-redundant operation of the FDC 157-0 DP/PA coupler, refer to manual *Bus links DP/PA coupler, DP/PA link and Y link*.

The figure below illustrates an example configuration and possible errors in a non-redundant PA segment, as well as their consequences and the severity of the damage which can be expected.

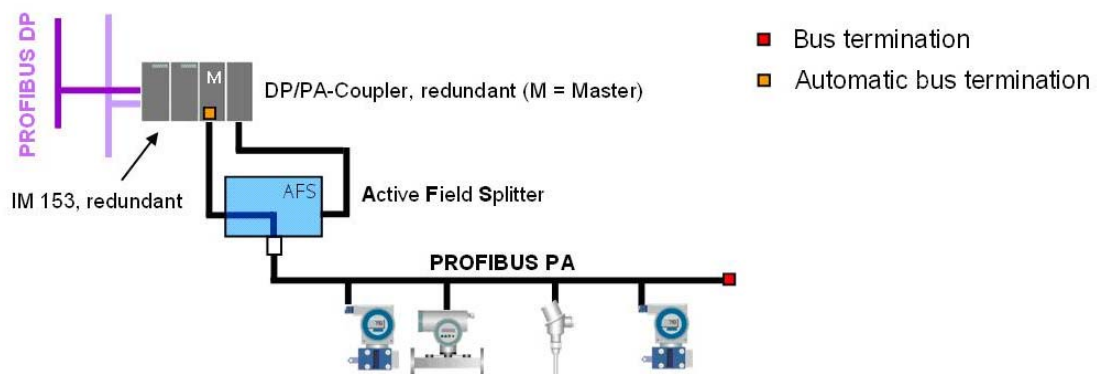


### PROFIBUS PA redundant configuration

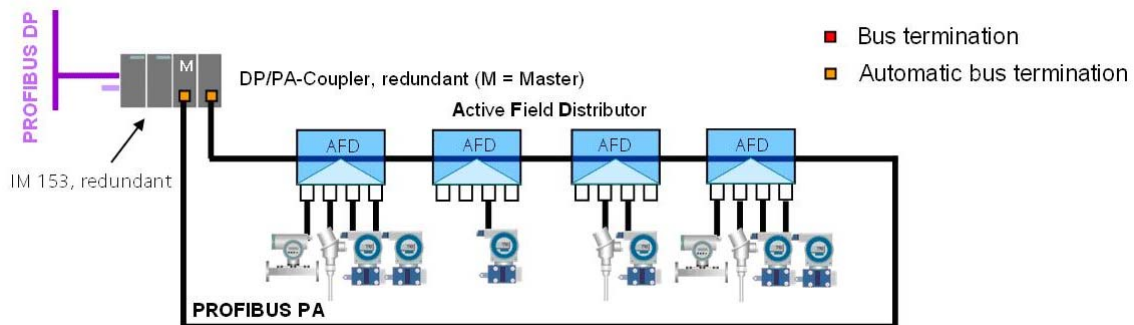
A PROFIBUS PA redundant configuration reduces the risk of plant failure by making it less likely that failure will occur in the first place, as well as restricting the extent of any damage that may occur. From a hardware/technical point of view, this redundancy concept is based on couplers and intelligent field distributors.

Basically, the two configuration versions below are available for redundant PROFIBUS PA:

#### Coupler redundancy



## Ring redundancy



The FDC 157-0 DP/PA coupler provides various items of diagnostic information.

### Note

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

### Connection of field devices in the hazardous area

Coupler redundancy can be used to increase availability, including for ex applications. Field barriers (e.g. Pepperl&Fuchs) can be used downstream of the AFS on the PA main line. These can be installed directly up to hazardous zone 1.

## 5.5.4 SIMATIC PDM

SIMATIC PDM (**P**rocess **D**evice **M**anager) is a software package for the configuration, parameter assignment, commissioning, and maintenance of devices (for example, transducers) and the project engineering of network configurations and PCs. Among other things, it enables process values and alarms, as well as device status information, to be monitored easily. Commissioning and maintenance are also supported by a LifeList program, which is able to read field device configurations online.

### Electronic Device Description (EDD)

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.

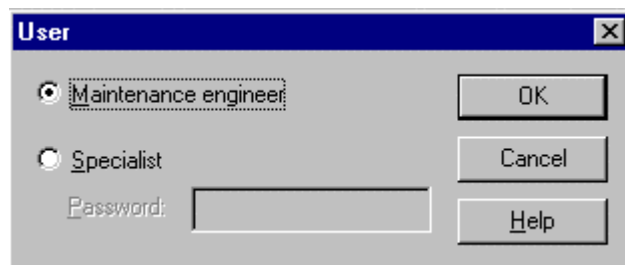
SIMATIC PDM is fully integrated in PCS 7. All devices integrated in a project using EDD can be parameterized, commissioned, and maintained from a central engineering station by means of a single tool.

## Change Log

The change log in SIMATIC PDM allows you to see at any time which user has made which changes in a project and when. This change log function helps to meet the requirements of authorities such as the FDA, which demand that changes in the production plant must be appropriately documented so that they can be traced back.

## Access Protection in SIMATIC PDM

Integrated access protection manages rights for changing the parameter assignments of field devices in SIMATIC PDM. In “maintenance engineer” mode, only changes which are required for operation and maintenance may be made in the parameter table. Advanced change options are made available in the parameter table for “specialists”. “Specialists” need to enter a password, previously defined in the settings, in order to log on.



## Export Functions in SIMATIC PDM

In SIMATIC PDM, the following field device data can be backed up via an export procedure:

- 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. In addition, a version can 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 (“PDMEExportEddl.XSL” for the device parameters and change log or “PDMEExportCalibration.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.

---



### 5.5.5 FOUNDATION Fieldbus (FF)

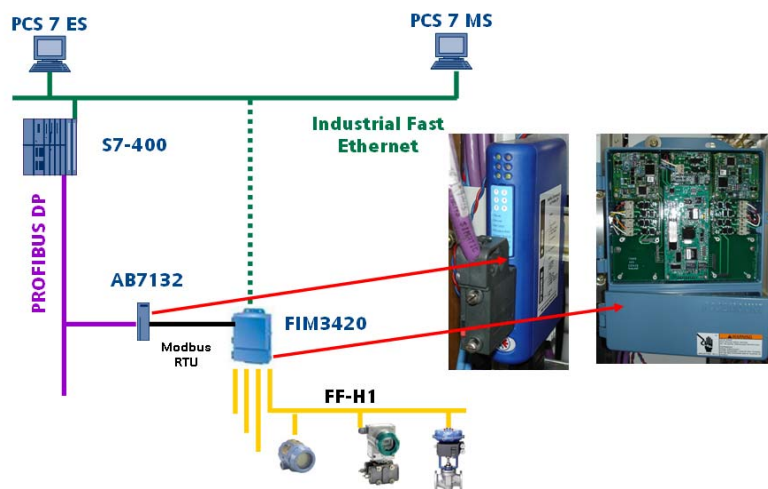
As well as facilitating communication via PROFIBUS or HART, SIMATIC PCS 7 also offers interfaces for FOUNDATION Fieldbus (H1), allowing a wide range of FF instruments and positioners to be easily integrated into the process control system. The FOUNDATION Fieldbus H1 is connected to PROFIBUS DP via the DP/FF link.

This concept offers:

- Central engineering of the DP/FF link and FF field devices without the need for additional tools
- FF drivers in the PCS 7 library and the support of the driver wizard
- Integration in PCS 7 Asset Management
- Cyclic and acyclic communication
- Cyclic diagnostic information provided by the DP/FF link and the FF field devices

A DP/FF link bundle consists of:

- AnyBus DP link AB7132 (HMS)
- Fieldbus interface module FIM3420 (Rosemount) with 4 FF H1 segments and integrated supply parts



The AnyBus DP link can be operated downstream of a Y link for connection to a redundant DP master system.

### Diagnostics with PCS 7 Asset Management

A diagnostic symbol is created on the PROFIBUS DP device level in the diagnostic area for each AnyBus DP link. It is advisable to insert a status indicator and a button for switching to the user diagnostics of the connected FF field devices for each AnyBus DP link.

## Configuration and Diagnostics via the FIM3420 Web Interface

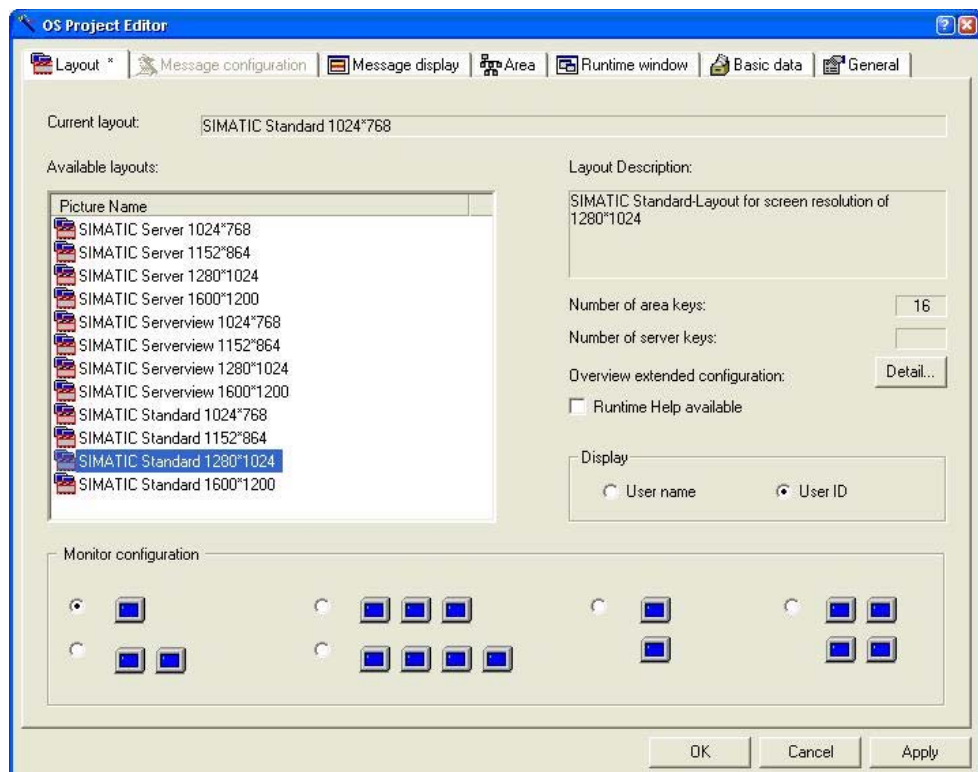
The FF field devices connected to the FIM3420 are configured and diagnosed via the Web interface supplied.

## 5.6 OS Project Editor

The OS Project Editor is the basic tool used for setting up the user interface, i.e. for setting the screen layout, screen resolution, etc. The requirements for the functionalities listed below are defined in the specifications.

- Creation of the PCS 7 event-signaling classes and message types
- Creation of the message blocks
- Creation of the PCS 7 messages
- Display of the PCS 7 messages
- Configuration of the startup lists and the start screen
- Copying of the dynamic wizards and the actions
- Layout of the hierarchical structure and the area to be displayed
- Number and display of the process windows
- Management of basic data such as pictures, actions, and libraries

When an OS project is created in the SIMATIC PCS 7 ES, the OS Project Editor is called in the background and initialized with default settings. Modifications due to customer requirements are made in the configuration of the Project Editor. The following screenshot shows the layout of the OS Project Editor.



Another specification made in this Project Editor is whether the user interface should display the “User name” or the “User ID”, for example.

## 5.7 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. In runtime, 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 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 belonging to the PCS 7 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 Workgroup

In a workgroup environment, the plant bus is synchronized via the central plant clock (SICLOCK, for example). The OS servers obtain the time from the plant bus; they are configured as “cooperative time masters”. If no SICLOCK timer is present, an OS server becomes the active time master. The automation stations obtain the time from SICLOCK; 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 loaded.

### Time Synchronization in a Windows Domain

If the automation system is operated in a Windows domain, the primary domain controller works as the time master on the terminal bus. It obtains its time from a SICLOCK connected in series, for example. The OS servers receive the time from this domain controller via the terminal bus. The OS clients obtain the time from a selected OS server. 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.

In case of stringent time stamping requirements, the automation stations also have to be synchronized directly by a SICLOCK TM via the plant bus.

If the plant uses components, such as BATCH servers, on which no operator station is installed, these must be synchronized additionally. This can be done via an additional DCF77 or GPS service or by means of software over the network or the Internet.

---

**Note**

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

---

**Note**

If a SICLOCK is used as the timer and the operator station display is adjusted to daylight-saving time, the SICLOCK must also be configured to daylight-saving time to ensure that all messages are archived with the correct time stamps. This adjustment must be activated on the operator station on the Control Panel > Date and Time > Time Zone tab.

---

**More Information**

Procedures for configuring time synchronization can be found in the following documents:

- Function Manual ***PCS 7 Time Synchronization***
- Manual ***PCS 7 V7.0 SP1 Engineering System***, section “Setting Time Synchronization”
- Manual ***PCS 7 V7.0 Operator Station***, section “Time Synchronization”
- Manual ***PCS 7 V7.0 High-Precision Time Stamping***
- Manual ***PCS 7 Security concept PCS 7 and WinCC***
- FDA Guidance ***21 CFR Part 11 – Time Stamps***, 2002, withdrawn

## 5.8 Configuration Management

The configuration of a process control system consists of various hardware and software components, which may be of varying complexity, from standard components through to specially customized user components. A clear and complete overview of the current system configuration must always be available. To facilitate this, the system is first divided into configuration elements, which can be identified by means of 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 3.1.

In terms of software, standard components include, for example, SIMATIC PCS 7 system software, associated libraries, other options, etc. As with hardware, these are also defined by and documented with their designation, version number, etc.

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 which the application software must be divided into, due to differing customer requirements and system designs.

### Versioning Configuration Elements

While users/project engineers cannot modify the version ID of standard software, application-software configuration calls for work instructions which specify, among other things, the assignment of version numbers and a change control procedure. All configuration elements must be maintained in a transparent manner, from the start of System Build onward.

---

#### Note

Examples of how individual software elements can be versioned are given in subsequent chapter 5.9.

Change control of various elements is explained in chapter 6.9.

More information on configuration control in PCS 7 can be found in chapter 7.4; with general information on configuration management available in **GAMP 4**, chapter 7.11.7 and Annex M9).

Changes made to a plant in operation should always be agreed with the process owner, see chapter 8.2.

---

## 5.9 Versioning Software Elements

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

“The main version is set to 1.0 following the FAT and to 2.0 following commissioning. All other changes are reflected by incrementing the sub 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).

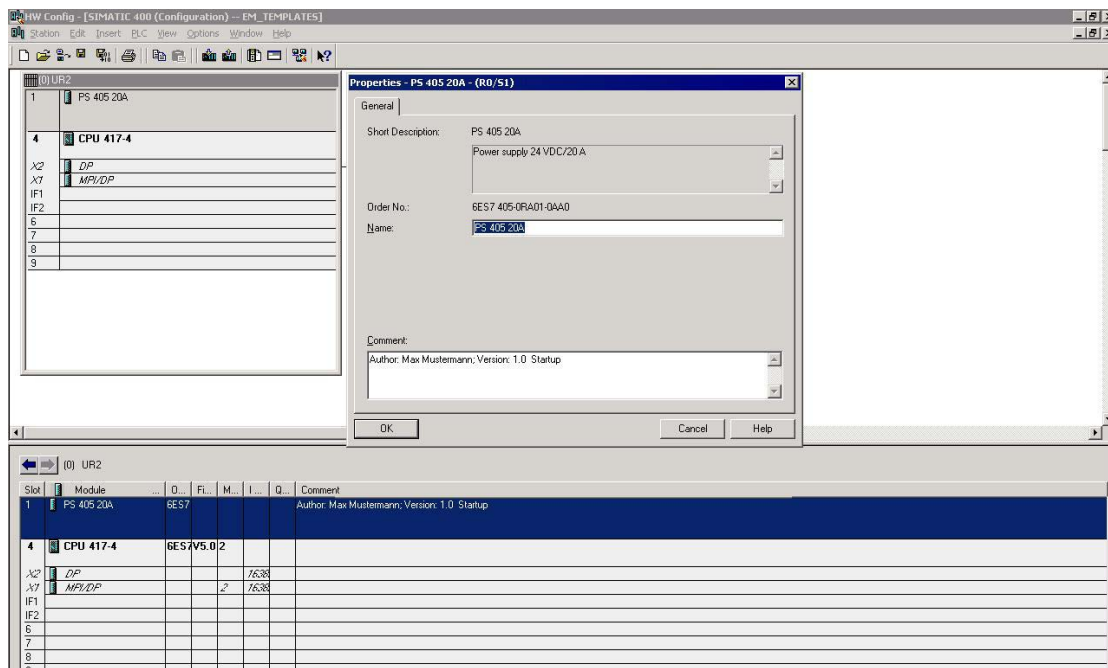
Various examples of software element versioning are given below. These are broadly divided into:

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

### 5.9.1 Versioning AS Elements in PCS 7

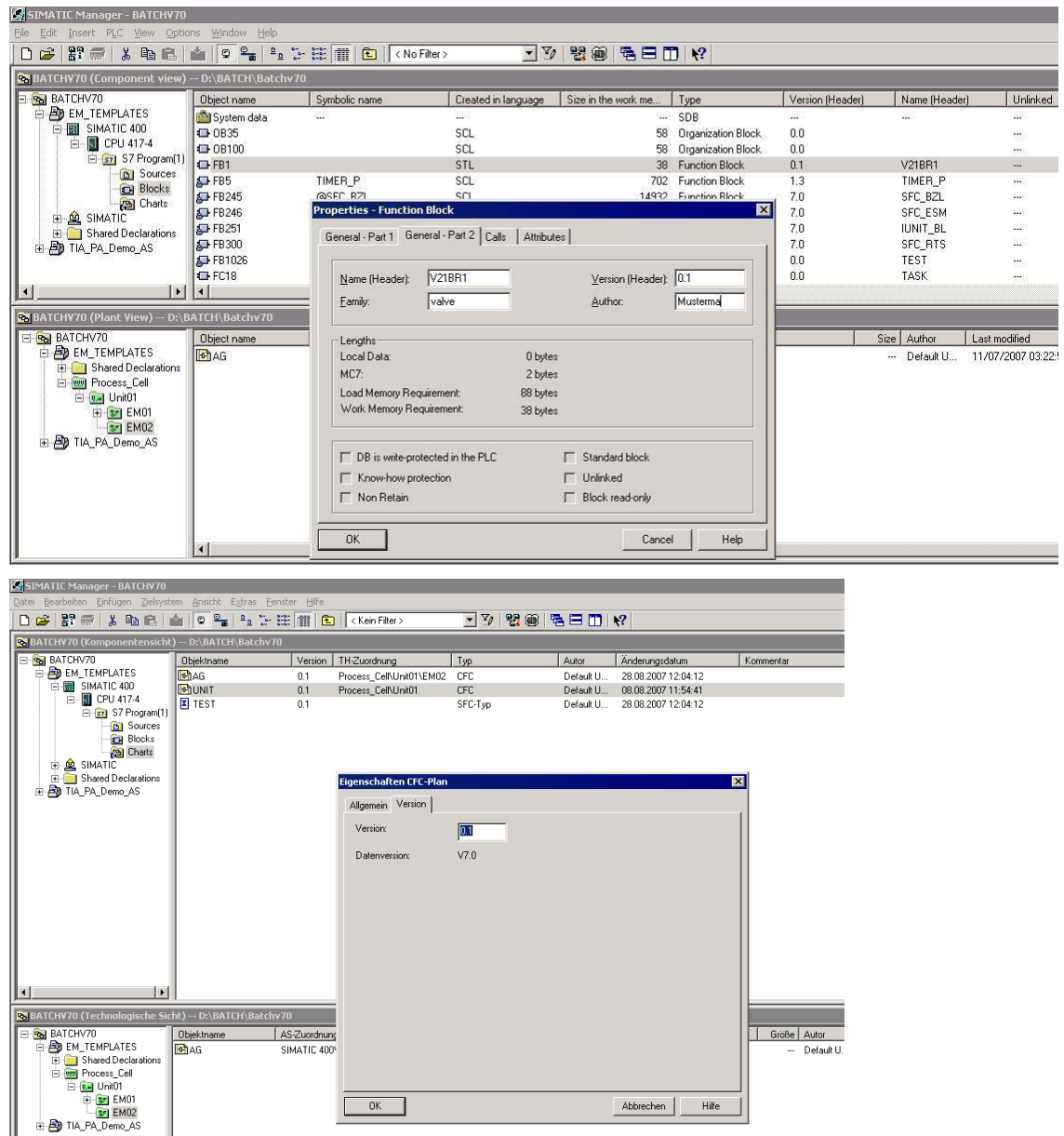
The individual configuration levels in PCS 7 provide different options for assigning version identification and, possibly, an author and comment to each element.

#### Versioning the Hardware Configuration in “HW Config”



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

## Versioning Blocks, CFC Charts, and SFC Charts



For blocks, CFC charts, and SFC charts, as well as for SFC types and models, version numbers are managed in the properties of the respective object, see graphic above.

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.

The screenshot shows the SIMATIC Manager interface with two windows open. The top window, titled 'CFC - [UNIT -- EM\_TEMPLATES\Process\_Cell\Unit01]', displays a version history table for the object 'V21BR1' (Description: Hot-water valve). The table lists two versions: V 1.0 (Author: M. Malte, Comment: New construction, Date: 2007-08-12) and V 1.1 (Author: P. Mayer, Comment: Expansion UNIT0 Block, Date: 2007-09-03). The bottom window, titled 'SFC - [TEST -- EM\_TEMPLATES\SIMATIC 400\CPU 417-4V...]', shows a ladder logic diagram with a 'START' button connected to a coil '1' and then to a contact 'ON'. A separate text box in the bottom right corner shows the version history for the 'Sequence Hot-water valve' object, listing V 1.0 (Author: M. Meyer, Comment: New construction, Date: 2007-07-25) and V 1.1 (Author: M. Malte, Comment: Expansion ON Function, Date: 2007-08-16).

Version	Author	Comment	Date
V 1.0	M. Malte	New construction	2007-08-12
V 1.1	P. Mayer	Expansion UNIT0 Block	2007-09-03

Version	Author	Comment	Date
V 1.0	M. Meyer	New construction	2007-07-25
V 1.1	M. Malte	Expansion ON Function	2007-08-16

The screenshot shows the SIMATIC Manager interface with the 'LAD/STL/FBD - [FB1 -- EM\_TEMPLATES\SIMATIC 400\CPU 417-4]' window open. The 'Interface' section on the left lists variables: IN, OUT, IN\_OUT, STAT, and TEMP. The main area displays the 'Contents Of: 'Environment\Interface'' table, which lists these same variables. Below this, the 'FB1 : Initialization' section is highlighted with a red box, showing the following text:

```

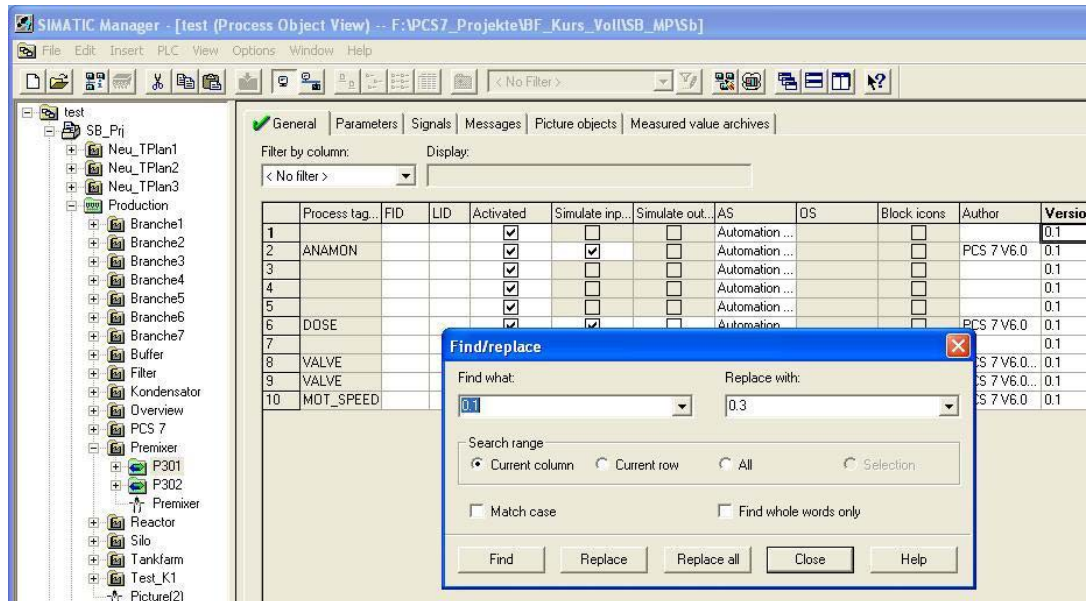
Author: Max Mustermann
Version: V1.0 2007-09-01
Object: V21BR1
Comment: Hotwater valve sequence
  
```

Below the initialization code, the 'Network 1: Declaration' section is visible, showing the text 'Definition global variable'.

### 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. Version and change comments must then be maintained in the unit CFC.





## Versioning the Configuration in SIMATIC NET

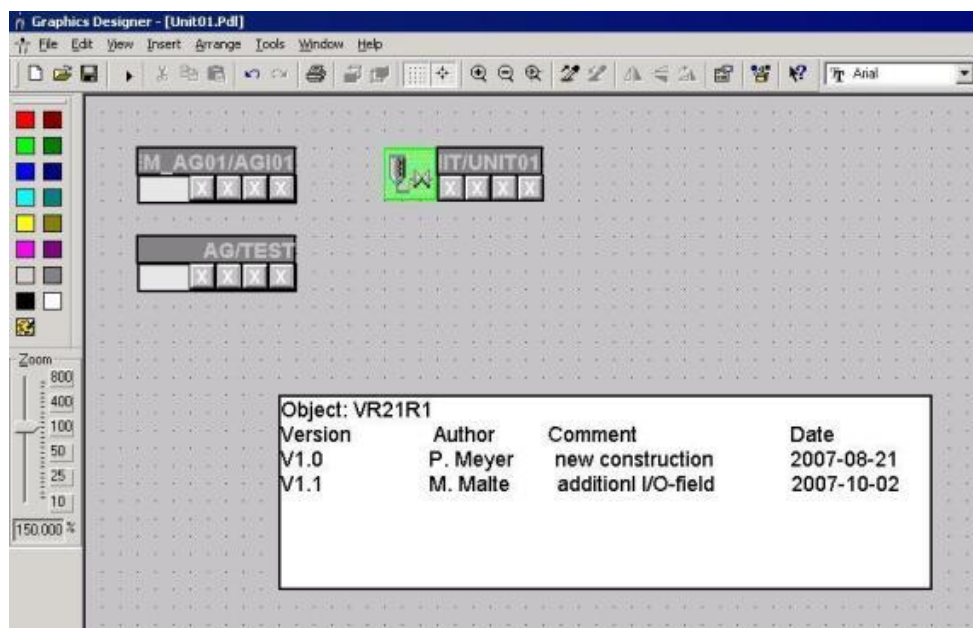
The version identification can be entered in the properties on the bus level (system bus, PROFIBUS).

## 5.9.2 Versioning 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 identification and comment must have been inserted in the script header in text format.

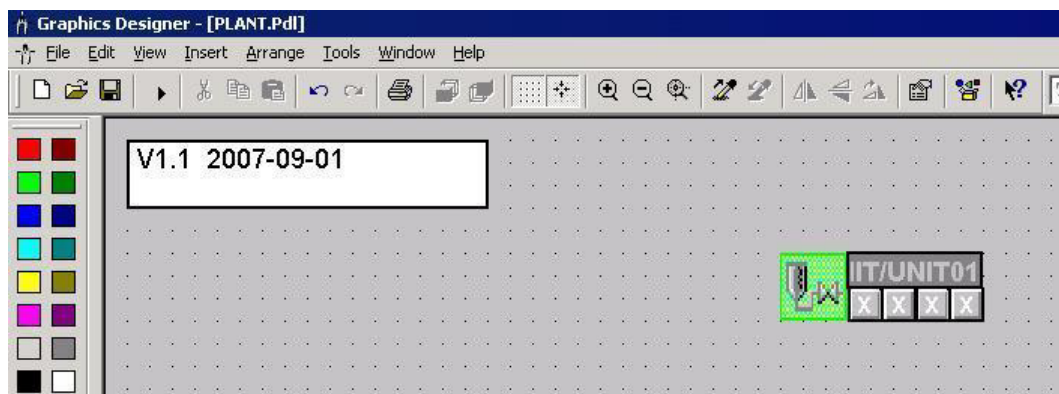
Configuration settings must be appropriately documented, on the one hand to act as a reference for use in validation/qualification, and on the other hand to ensure they are available if the system needs to be restored.

### Example for Graphic Displays

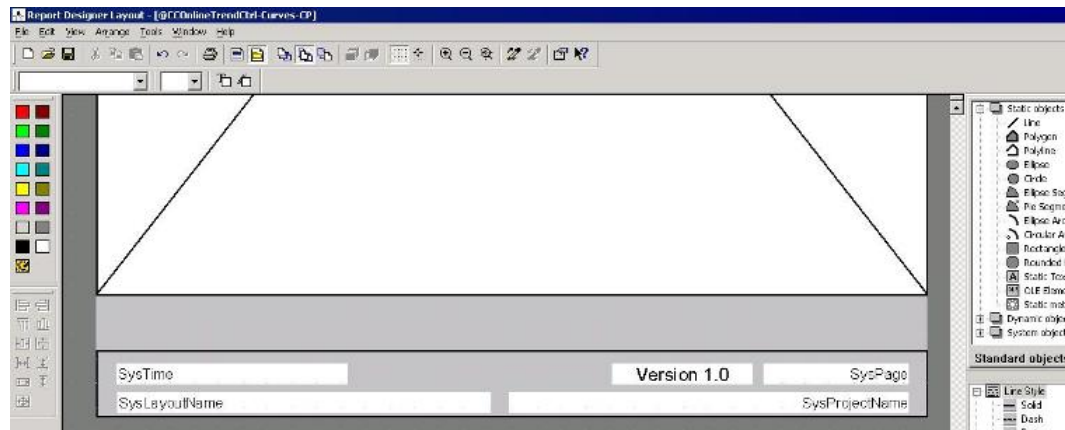


Upper graphic: Versioning in a hidden field within the graphic display

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

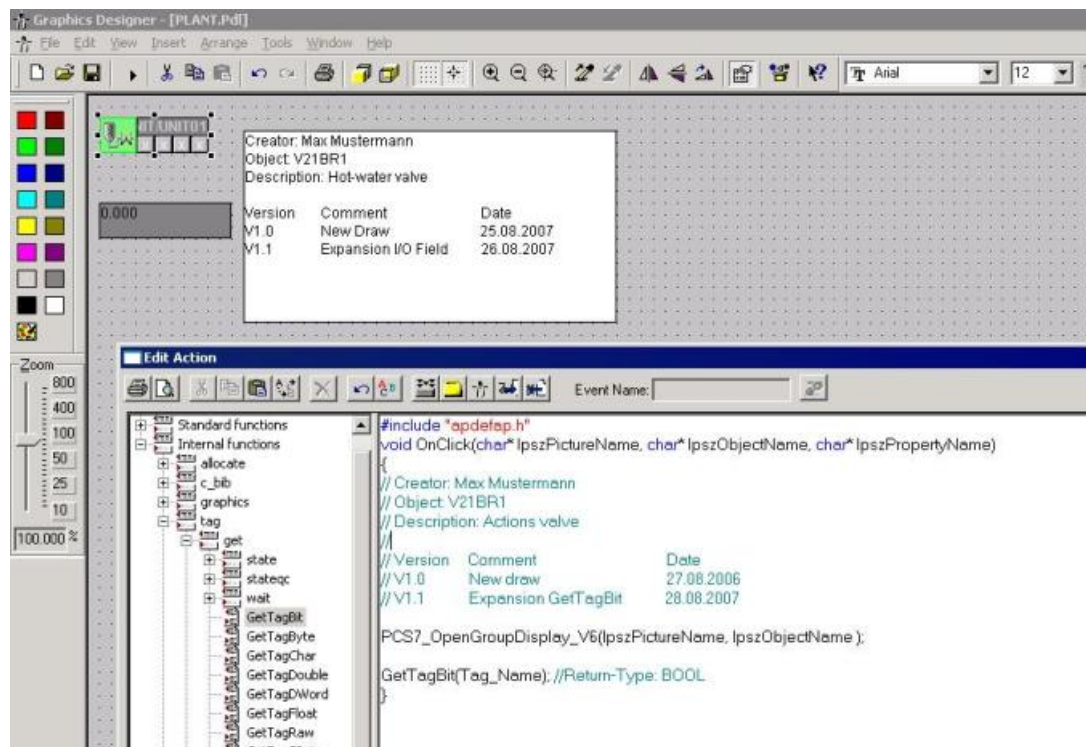


## Example for Reports



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

## Example for C/VB Scripts



Version and comments added within the script

### **5.9.3 Further Information on Versioning**

#### **Versioning BATCH Elements**

Recipe versioning is described under “Change Control for Recipes” in chapter 6.9.3.

#### **Versioning Projects, Multiprojects, and Libraries**

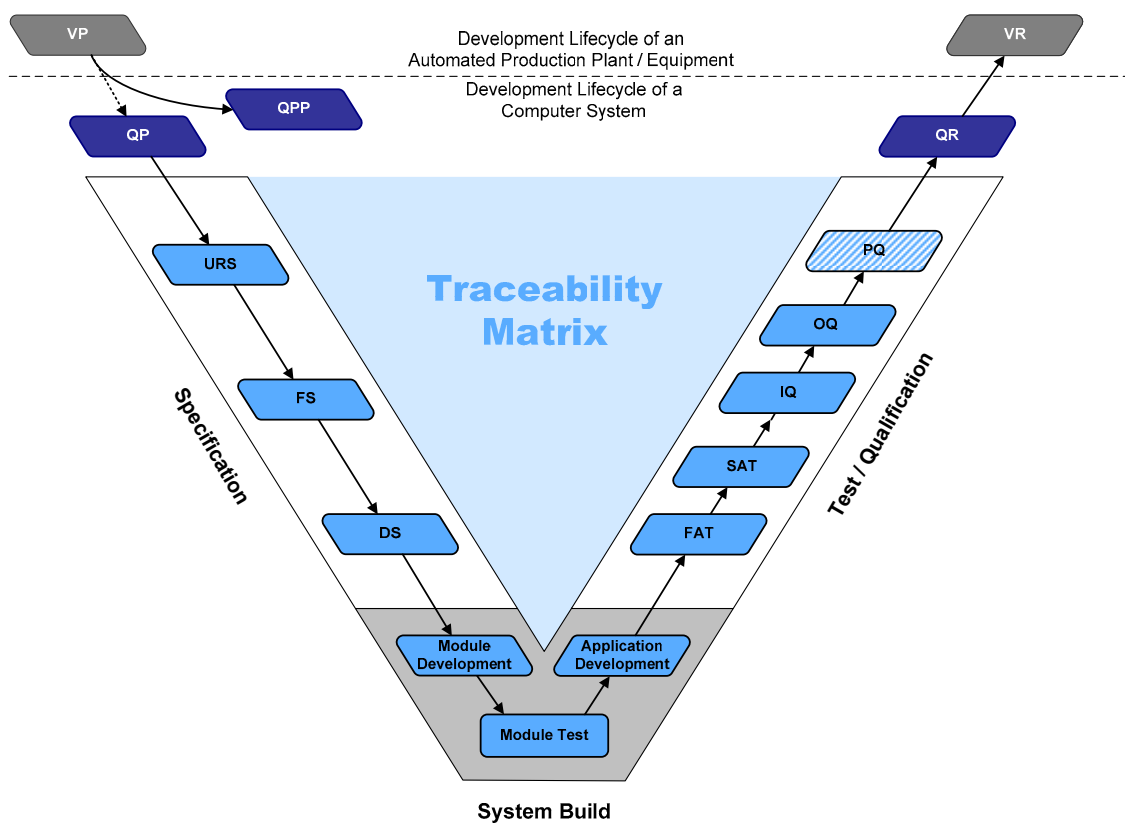
Supporting system functions for versioning projects, etc. are described in chapter 7.4.



## 6 Creating Application Software

This section describes the creation of application software in the GMP environment.

In the following graphic the highlighted area at the bottom illustrates the phase of the System Build, where the activities of this section belong to.



## 6.1 Software Modules, Types, and Typical

The use of software modules and typicals is common in process control engineering. They are used in the form of function blocks, function charts, or complex sequencers, which can be duplicated within projects.

### Note

Modules and typicals 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.

### 6.1.1 Modules and Typicals in PCS 7

A distinction is made in SIMATIC PCS 7 between an SFC type, a process tag type, and a model.

<b>SFC type</b>	<b>Interface to SIMATIC BATCH for operating equipment phases / equipment operations, for example:</b> <ul style="list-style-type: none"> <li>• Heating</li> <li>• Stirring</li> <li>• Draining</li> </ul>
<b>Process tag type</b>	<b>A CFC chart, for example:</b> <ul style="list-style-type: none"> <li>• Valves</li> <li>• Pumps</li> <li>• Motors</li> </ul>
<b>Model</b>	<b>Combination of several CFC and/or SFC charts, for example:</b> <ul style="list-style-type: none"> <li>• PID temperature control of a tank</li> <li>• Level monitoring including safety shutdown to prevent tank overflow</li> <li>• Unit</li> </ul>

The mode of operation of the modules must be described in a specification in which the parameter assignments (MES-relevant, archiving, block comment, unit of measure, etc.) and interconnections are defined. More detailed information about how to use software typical while programming can be found in chapter 2.4.

---

**Notes**

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

The modules/typical 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 in the form of a document, containing the respective software version for each AS.

---

**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. an SFC type cannot access just any process signals, in contrast to an SFC chart.

More detailed information can be found in the manual **SFC for SIMATIC S7**.

Alone, the SFC type cannot execute. An SFC type, just like a function block type, must be placed in a CFC chart before it receives an executable object, in this case an SFC instance. The SFC type and SFC instances are compiled when the program is compiled. To run an SFC instance, both the SFC type and the SFC instance are downloaded to the automation system.

**Process Tag Type / Model**

With SIMATIC PCS 7, a process tag type/model consisting of one or more CFC and/or SFC charts can be created for subcomponents of the same type. Creating process tag types or models for similar plant units saves on engineering and testing effort. Once a process tag type or model has been tested, it can quickly be duplicated as often as required in the multiproject in the form of replicas. For each replica, the plant hierarchy, CFC name, messages, I/Os for parameters or signals, and various module properties can be adapted.

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. Models can contain pictures and reports.

---

**Note**

See chapter 6.1.3 for information on using block icons. These should be tested together with the associated software module as a process tag type and approved by the customer before they are duplicated.

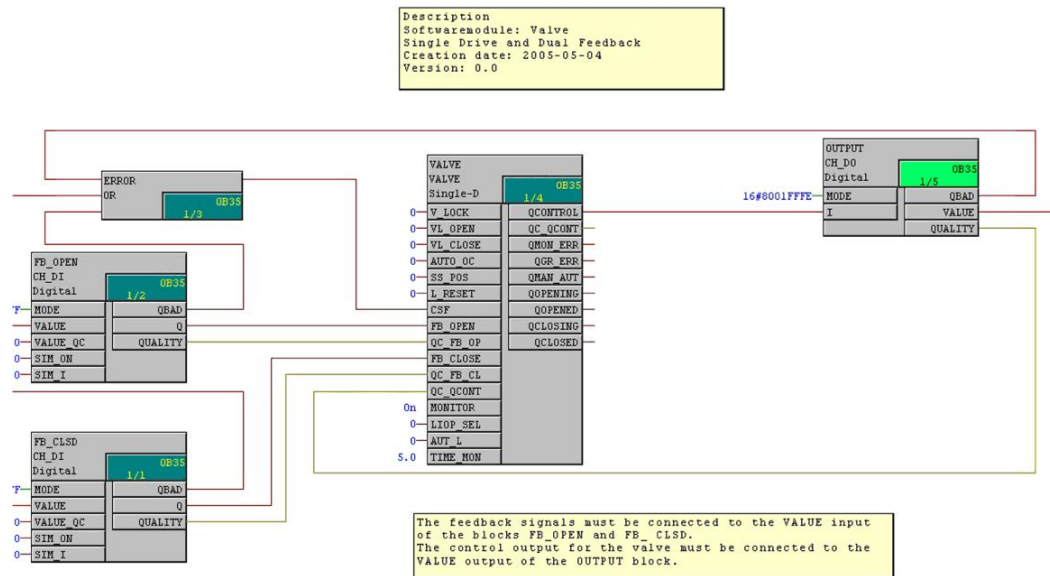
---



### 6.1.2 Example of a Process Tag Type

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

For a spring-closing valve, the module might appear as shown below.



The valve to be controlled features a control signal for the OPEN function and two feedback messages for the statuses opened and closed, as well as monitoring of module peripheral faults for the statuses feedback message open/closed. Blocks from the PCS 7 standard library were used for the example above.

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").

#### Note

When creating the process tag type, also some settings can already be defined, e.g. the settings for process value archiving.

### 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 allows several template pictures to be used.

#### Note

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

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 template pictures, and automatically linked to the tag interface of the relevant operator panel.

Priority	Picture name	Remarks
1	@PCS7Typicals*.pdl	Starting alphabetically reverse
2	@PCS7Typicals.pdl	
3	@@PCS7Typicals.pdl	Contained in the standard

### The @@PCS7Typicals.pdl Template Picture

The “@@PCS7Typicals.pdl” picture is included in every PCS 7 OS project by default and contains standard block icons.



#### Note

The “@@PCS7Typicals.pdl” original file must not be changed under any circumstances! Any changes to the original file will be overwritten when an update or upgrade is performed.

For customer-specific block icons separate template pictures should be created, “@PCS7Typicals\*.pdl”, see also FAQ 26697820 und 19688107.

### Project-Specific Template Picture

A project-specific template picture, “@PCS7Typicals\*.pdl”, can be created by copying template picture “@@PCS7Typicals.pdl”. Customer-specific changes can then be made to the “new” template picture.

### The @Template.pdl Template Picture

The “@Template.pdl” template picture 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.

Nevertheless, it can be beneficial 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 “@Template.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 “@Template.pdl” file on a regular basis.

## Further Template Pictures

**@@ConfigTypicals.pdl**

Used to create/update lifebeat monitoring

**@@MaintenanceTypicals.pdl**

Used to create/update diagnostic pictures

**@pcs7elements.pdl**

The template picture 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. 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.

---

## 6.2 Bulk Engineering with the IEA

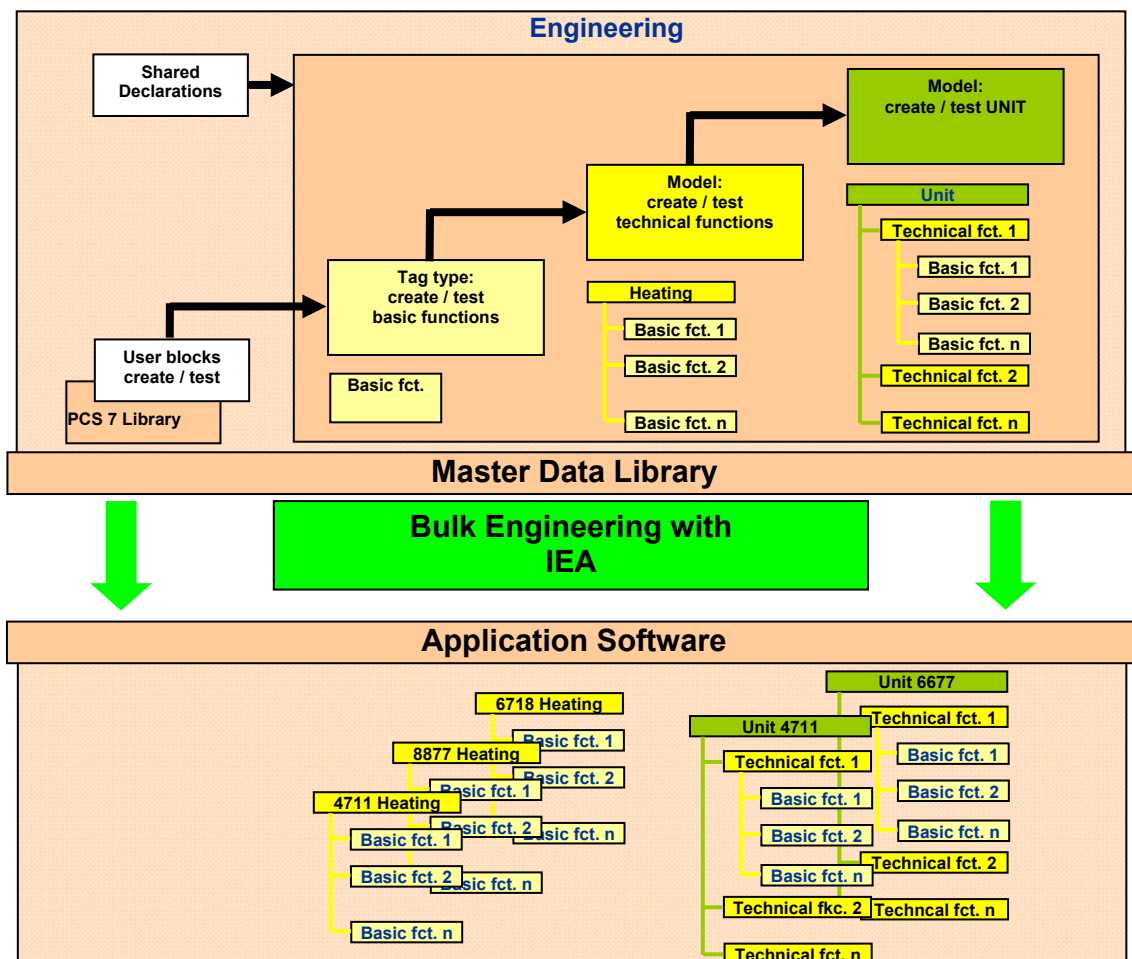
The Import / Export Assistant (IEA) is used for two tasks.

### Multiplication with the IEA

The Import/Export Assistant is used to duplicate process tag types or models several times. This is achieved by defining project-dependent typical on the basis of standard libraries; these typical can then be copied as often as required by using the Import/Export Assistant to perform instantiation. You will find an example in chapter 6.2.

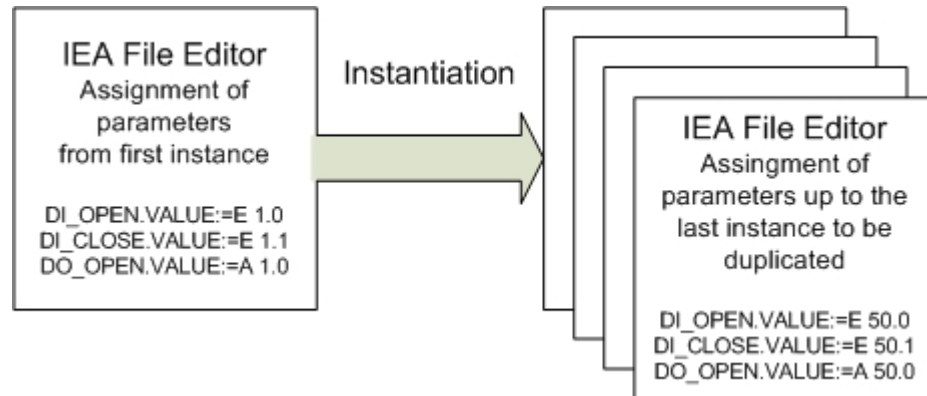
#### Note

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



## 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.




---

### Note

The IEA is an optional package in SIMATIC PCS 7. It is included on the *PCS 7 Toolset DVD* and installed as part of the common setup, but it does require a separate license.

---

## 6.3 Creating Process Diagrams

See chapter 6.1.3 for how to use template pictures as a library for graphic typicals.

Process diagrams must be created in accordance with the definitions contained in the specifications (e.g. URS, FS, and P&I).

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

Once the graphics have been created, they should be shown in the form of screenshots to the customer for approval.

## 6.4 User-Specific Blocks and Scripts

User-specific blocks (FB, FC) and scripts (C, VB) are assigned to GAMP Software Category 5, see chapter 7.3.1. This type of software is developed to meet customer-specific demands not covered by existing libraries.



---

### Notice

The creation of category 5 software should be avoided because it significantly increases the testing and validation work required.

---

The procedure for creation of **Category 5** software is as follows:

3. Creation of a functional description for the software
4. Specification of the function blocks used
5. Specification of the inputs and outputs used
6. Specification of the operator control and monitoring capability
7. Creation of software in accordance with specifications and programming guidelines
8. Testing of the structure for compliance with programming guidelines
9. Testing of the function for compliance with the functional description
10. Approval prior to use and/or duplication

## 6.5 Interfaces to PCS 7

### 6.5.1 PCS 7 OS Web Option

This option enables PCS 7 system process operation to be controlled and monitored via an Internet/Intranet connection. One PCS 7 OS Web server and at least one PCS 7 Web client are 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 be used as an operator station (OS client); this can be ensured by deactivating graphics runtime.

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 using the "Web View Publisher".

---

#### 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, if necessary.

The manual **PCS 7 OS Web Option** provides information on the script functions which are supported.

---

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

At the PCS 7 Web client, the operator can log on via Internet Explorer and a TCP/IP connection and access data on the OS Web server. The user interface shown in Internet Explorer looks like that of any "normal" operator station (OS client), with overview, working, and button areas. The logon via a Web client is entered in the Web server's Windows EventLog, with the relevant user ID also being specified.

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 rights are assigned in WinCC user administration. They correspond to those of standard clients, the only additional adjustment is that the Intranet/Internet access option must be enabled.

All operations performed by the operator on the Web client are logged automatically with the name of the operator. In contrast to standard clients, the Web client does not support automatic logoff. However, a password-protected screensaver or a work instruction on how to terminate the Web connection can be used to provide appropriate access protection support for the Web client.

Status information on which user is logged on to a Web server and from which Web client can be called from the OS Web server or any Web client. There is one information block relating to the OS Web server and one for each connected Web client, which provide the following data:

- Software version of the OS Web server installed
- Number of Web clients which access the OS Web server

- Users currently logged on and information relating to which Web client they are logged on via

Further information about Information Security can be found in chapter 4.6 of this document as well as in the manual **PCS 7 Security concept PCS 7 and WinCC**.

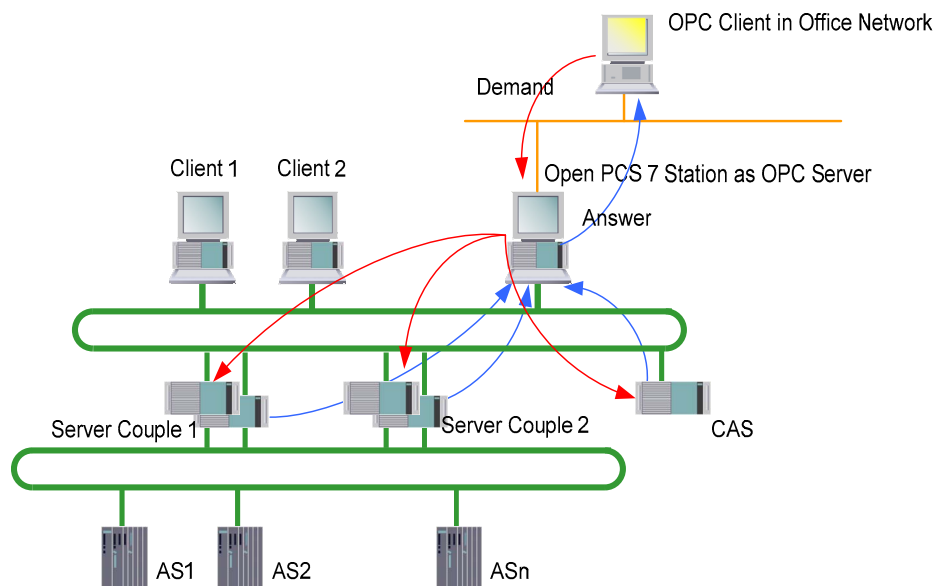
## 6.5.2 Open PCS 7

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 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, facilitates OLE/DB 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 a server fails, the Open PCS 7 station performs redundancy failover automatically. If the active server fails, the station switches to the remaining server automatically, so that this server carries out the next read job. An uninterrupted read job is repeated on the server which is then active.

The figure below shows a multiple station system with a client/server architecture. The Open PCS 7 client station is equipped with two network adapters. OPC client PC requests in the office network are clearly transferred out of the Open PCS 7 station to the OS server or the central archive server (CAS), which responds to the request.





Access to the station	OPC interface	Data type	Access method
OS server	DA	Tags in process mode	Read and write
OS server	A&E	Alarms and messages (Alarm Logging)	Read and acknowledge
OS server	HDA	Historical process values (Tag Logging)	Read
OS server	H A&E	Historical alarms and messages (Alarm Logging)	Read
CAS	HDA	Historical process values (Tag Logging)	Read

### 6.5.3 SIMATIC BATCH API

The SIMATIC BATCH application programming interface (API) is an open interface, which facilitates access to SIMATIC BATCH data and functions.

## 6.6 Integrating SIMATIC BATCH

### 6.6.1 Batch Definition of Terms

Commonly used batch terminology is described below.

#### **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

#### **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

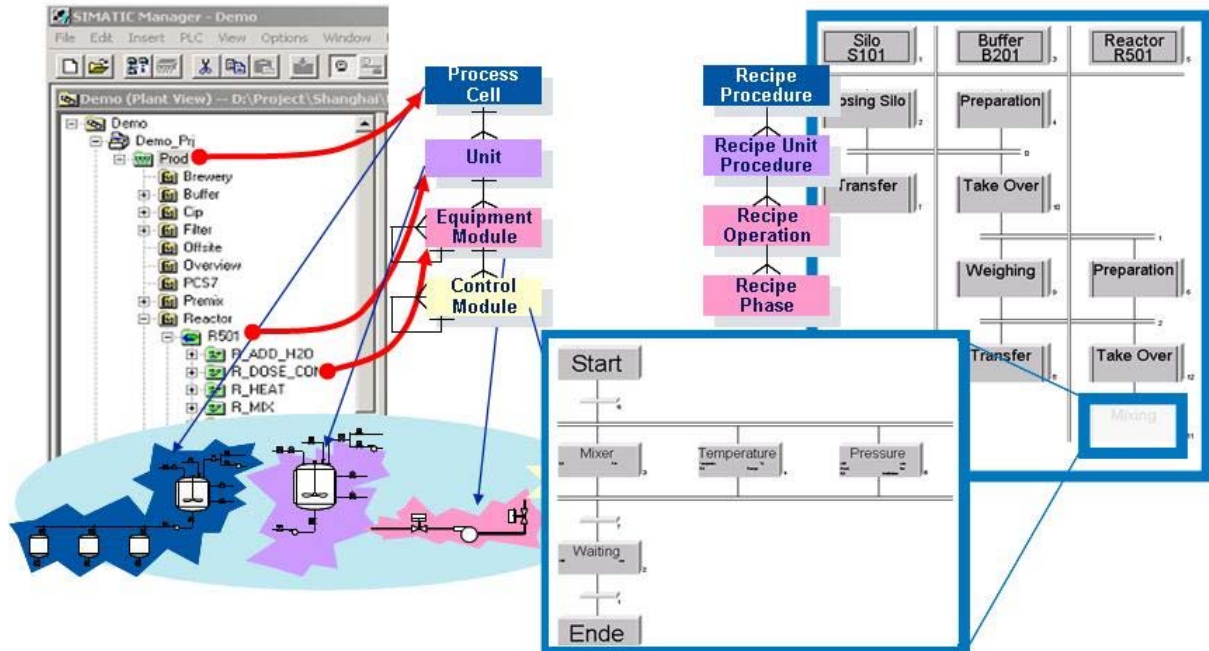
### 6.6.2 Conformity with the ISA-88.01 Standard

ISA-88 is an international standard. The standard ensures that equipment and software are flexible and can be reused. SIMATIC BATCH was developed on the basis of *ANSI/ISA-88.01 (1995) Batch Control, Part 1: Models and Terminology*.

One of the recommendations contained in the "Technical Report" *ISA-TR88.0.03-1996* is the use of SFC (Sequential Function Charts, DIN/IEC 1131) as a graphic language for describing recipe procedures. Recipes created with the BATCH Recipe Editor follow the structures and functionalities described in this standard.

### 6.6.3 ISA-88.01 - Software Model SIMATIC PCS 7

ISA-88.01 describes different 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 control-loop level, which is mapped using the plant hierarchy in the plant view of the 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.

#### Recipe Procedure

A recipe procedure runs on 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



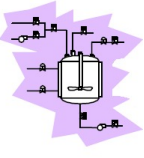
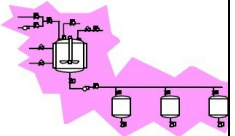
A recipe operation or a recipe phase runs on an equipment module to implement a process engineering task or function.

#### 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.

### 6.6.4 Implementing the ISA-88.01 Concept

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

Physical model	Graphics	Procedural elements	Implementation in PCS 7	Implemented by
Control Module (CM)		-	CFC component: Use of the PCS 7 library and of CFC charts	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 user
Unit		Unit procedure(s)	CFC component: Unit block Batch unit recipes	User / supported by supplier
Process Cell		Procedure	Batch component: Recipe	User / supported by supplier

#### SIMATIC BATCH can be integrated in two ways:

- Equipment phase with SFC types  
The SFC type or the instances of SFC types are the preferred interfaces of PCS 7 / SIMATIC BATCH.
- Equipment phase using SFC and interface blocks IEPH/IEOP  
These are interface blocks, which are used to control the process run. They must be inserted upstream of the processing block in the sequences in the CFC chart.

#### Note

The manual **Getting Started SIMATIC BATCH**, Part 3 and Part 4, describes the interaction between the individual levels (control-loop level and phase) and the equipment phases mentioned above.

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

### 6.6.5 Configuring SIMATIC BATCH

The manual *Getting Started SIMATIC BATCH, Part 2*, describes the configuration steps in detail.

Configuration can be divided into the following steps:

#### Working in the SIMATIC Manager

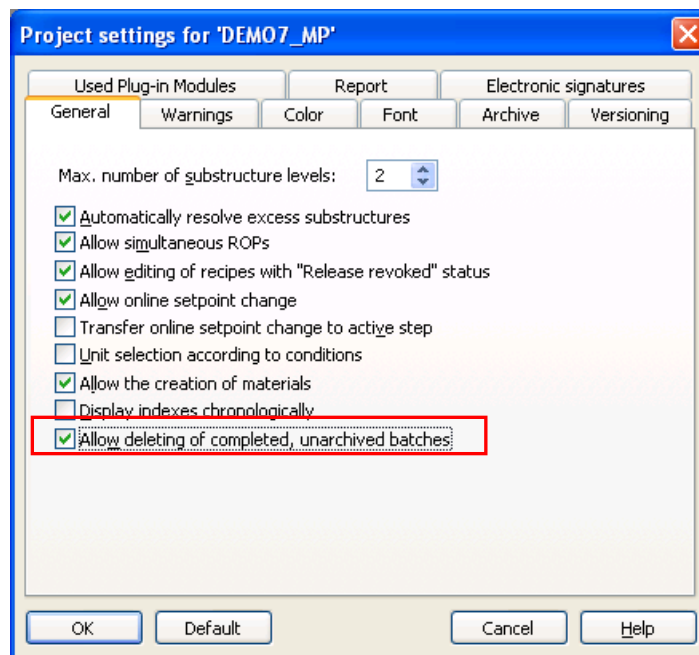
- Creating and configuring batch systems
- Creating the plant hierarchy
- Compiling OS data
- Generating batch types (SFC type)
- Propagating batch types
- Compiling instances
- Transferring data to OS
- Downloading process cell data

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

- Reading in batch data
- Creating master recipes
- Creating the recipe structure
- Releasing master recipes for production
- Creating an order
- Releasing a batch
- Creating ROP libraries (typicals)
- Exporting/importing recipes, parameter sets, etc.

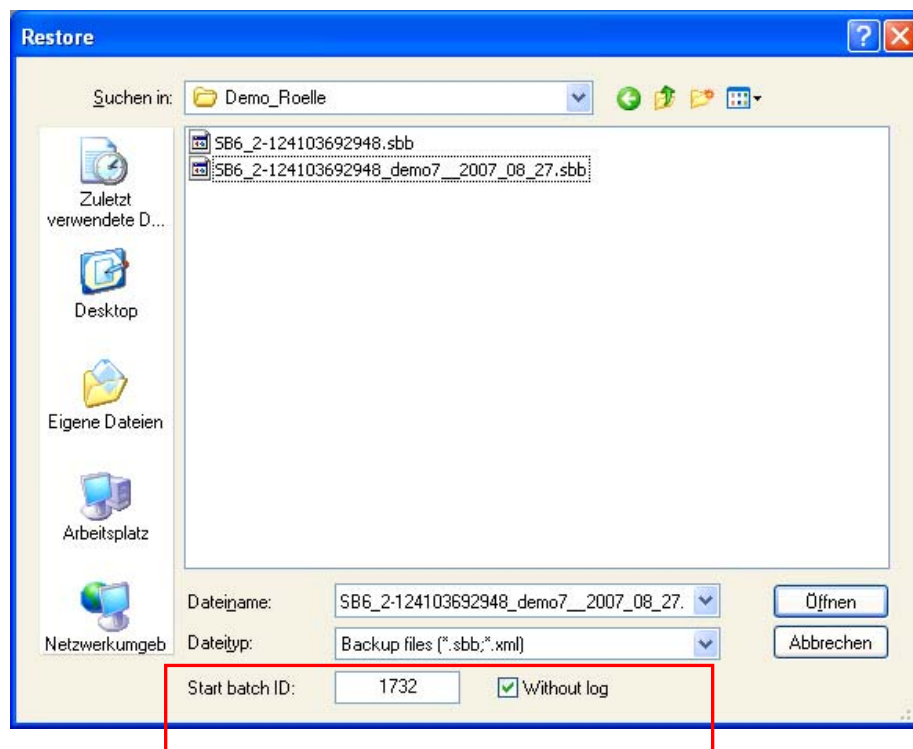
#### Project Settings in SIMATIC BATCH

Various project settings can be defined in SIMATIC BATCH. These settings are described in detail in the relevant system documentation. Particular attention should be paid to the point “Allow deleting of completed, unarchived batches”, for example. This function is needed only rarely in the pharmaceutical business and it should therefore be deselected, unless the customer explicitly requires this behaviour; see graphic below (where the option is still enabled).



### Backup/Restore for the SIMATIC BATCH Database

When a BATCH database is read in, a start batch ID can be assigned; this prevents batch IDs being assigned more than once. Whether or not the associated log is also to be imported is defined in this dialog box too.



## 6.6.6 Creating Batch Reports

The batch data stored by SIMATIC BATCH in XML format can be archived or processed with a report system for batch reports. The XML files are protected by checksums.

### Note

The choice of an archiving format and the desired creation of reports depend on the respective system constellation. Therefore this cannot be recommended in general at this place.

The batch data is available either as a file in an area “protected” by Windows security mechanisms on the hard disk or in a database and can only be accessed by authorized persons or systems.

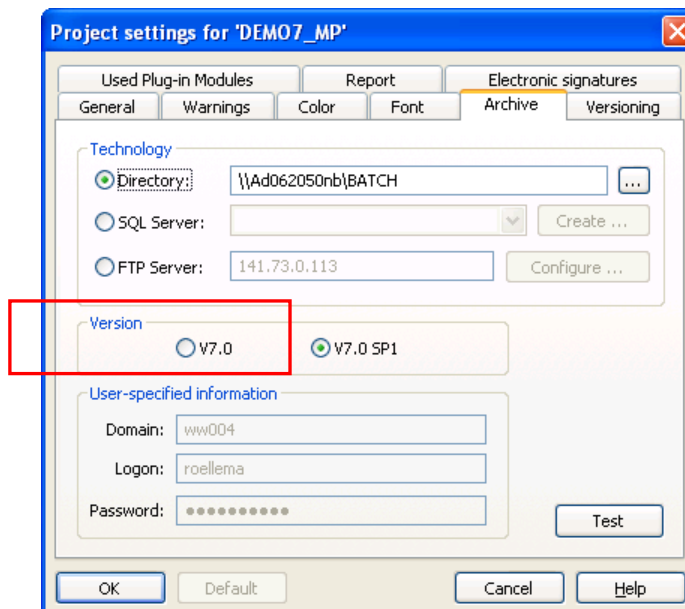
SIMATIC BATCH provides several ways of logging recipes and batch data, these are

- Standard report
- Advanced report based on a template
- Configurable advanced report

The user can switch between the standard and the advanced report at will, but the archiving format must be taken into account.

### Standard Report

Archiving format V7.0 must be selected in order to use the standard report, as it is created based on this format.



The figure below shows an example of how a standard batch report is structured.

**SIMATIC BATCH**

Batch / Batch ID	Batch1 / 8	Printed	Montag, 11. Juni 2007 14:05:10 +02:00	Batch log
Product / Code / Quality	Piccata Milanese / 47 / -	Page	1/10	

Status	completed + changeover + closed
Desired qty.	10 kg
Recipe / Version	Piccata / V1.0
Formula category	-
Formula / Version	- / -
Product order	today
Duration (setfact)	10 (s) / 10:02 (mcs)
Run time	2007-06-11T13:49:08+02:00 / 2007-06-11T13:59:10+02:00

**No. of events:**

	Unit	Error	Op. intervention	Limit value violation
Summary		0	11	0
Batch1		0	2	0
RUP	Pot_2	0	9	0
RUP	Oven	0	0	0

Batch		Batch1 (1) [0]				
		Run time		Act	Chart	Deviation
Step no.	Name	2007-06-11T13:49:08+02:00	2007-06-11T13:59:10+02:00	10:02 (m:s)	10 (s)	09:52 (m:s)
10000	● RUP	2007-06-11T13:49:09+02:00	2007-06-11T13:59:05+02:00	09:56 (m:s)	10 (s)	09:46 (m:s)
20000	● RUP	2007-06-11T13:49:09+02:00	2007-06-11T13:49:10+02:00	0 (s)	0 (s)	0 (s)

**Messages:**

Time	Source	Event
------	--------	-------

## Advanced Report Based on a Template

The appropriate entry must be selected in order to use the advanced report.

**Project settings for 'DEM07\_MP'**

General Warnings Color Font Archive Versioning

Used Plug-in Modules Report Electronic signatures

☒ Use advanced report

If you want to use the advanced report, ensure that the 'BATCH Advanced Report' add-on package is installed on the server.

Current server: AD062050NB

Check installation

Template for generating report:

standard

Default directory for PDF files:

\\Ad062050nb\BATCH

☒ Name and directory of PDF file can be changed

OK Default Cancel Help

The advanced report is created as a PDF file using Crystal Reports and archived in the same format. Predefined templates are used to create the report.



## Configurable Advanced Report

In addition to the standard layout for the advanced report, customer- or project-specific templates can also be created. A separate license is required for Crystal Report Designer in order to use this feature.

## 6.7 SIMATIC Route Control

SIMATIC Route Control is used to automatically transport materials and products within a plant.

### Fields of Application

Material handling deals with all products conveyed from the source container to the destination container on one hand, but also with highly complex cleaning procedures on the other.

### Hardware

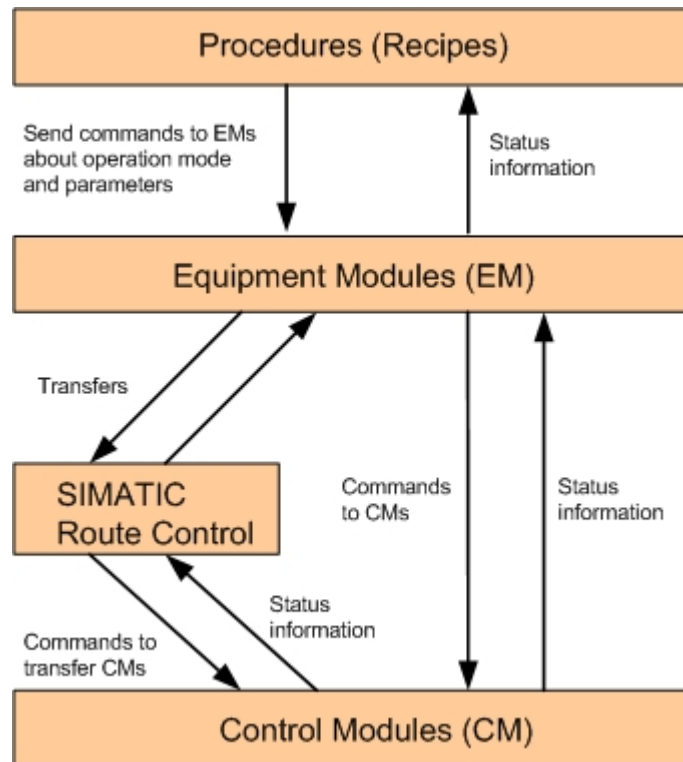
A Route Control server is needed in order to use SIMATIC Route Control. Route Control servers can have a redundant configuration. SIMATIC Route Control is configured in the SIMATIC PCS 7 engineering station.

### Software

SIMATIC Route Control is installed as an optional package and found on the SIMATIC **PCS 7 Toolset DVD**. SIMATIC Route Control uses the following SIMATIC PCS 7 software components:

- SIMATIC Logon; the user roles and access rights for SIMATIC Route Control are predefined and must be taken from the operator's manual.
- SIMATIC CFC chart for configuring path blocks for control modules
- SIMATIC SFC type for configuring automated materials handling for equipment modules
- SIMATIC NetPro for configuring S7 communication
- PCS 7 OS for configuring SIMATIC Route Control messages

## Interaction of the PCS 7, BATCH, and Route Control SIMATIC Components



In the context of an order, SIMATIC BATCH sends control commands to the equipment modules of the units on which production is to take place.

The equipment modules manage the control modules in the form of equipment phases. This is the standard way in which SIMATIC BATCH works.

If SIMATIC Route Control is used, it organizes and controls all transfers. This means that the transfer control modules are controlled and managed within SIMATIC Route Control.

Process states run in the opposite direction.

## Advantages of Using Route Control

If products are transported through different units in a process engineering plant (fermenter lines, for example) this means that equipment modules with different control strategies are configured for every outgoing and every incoming container transfer procedure as well as for the associated paths. Depending on the size of the plant and the number of transfer procedures, this can prove very time-consuming. Furthermore, the equipment module control strategies and the way in which they are synchronized between transfers and their interlocks have to be configured and verified by means of laborious tests.

If SIMATIC Route Control is used, every transport path is statically defined within it. SIMATIC Route Control uses the statically defined transport paths. When a path is specified, the source, destination, and partial paths are dynamically combined to give a complete path, taking the particular start conditions into account. If problems occur during transport, defined safe states are entered.

In addition, SIMATIC Route Control is integrated in SIMATIC BATCH, so also recipes which are not plant-specific can be configured. If plant units are occupied by a SIMATIC BATCH order, information on the destination and the source is supplied to SIMATIC Route Control, which enables the path to be dynamically compiled.

## 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 properties 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 message line and message page
- Event-signaling classes, colors, and priorities
- Acknowledgment concept (e.g. single acknowledgment)
- Event texts, e.g. "too high" for an upper 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 default standards for displaying event-signaling classes, colors, and priorities should be retained if possible and only be changed if a customer requests it.



#### Note

If the alarm system configuration differs from the standard configuration, the differences must be documented and an update procedure described; see also chapter 9.2.

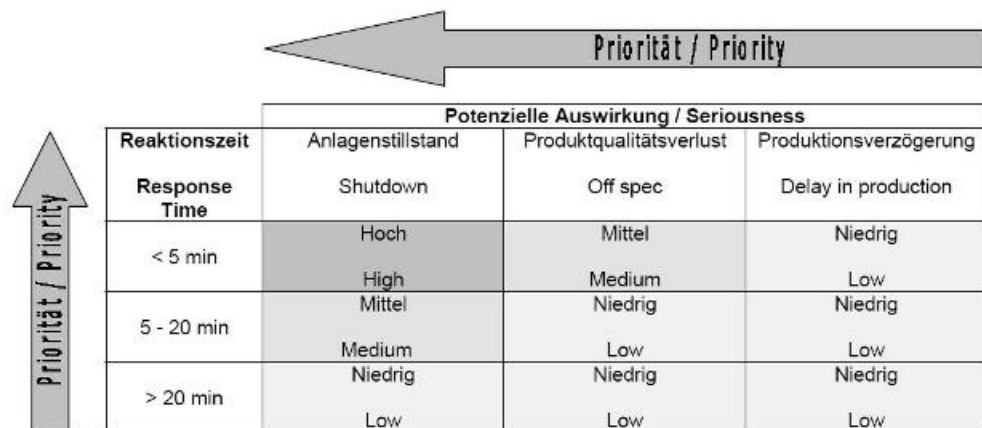
---

### 6.8.2 Event-signaling Classes

The different event-signaling classes, such as problem, 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 upper limits will trigger an alarm, the lower limits a warning, and a runtime error on a valve, for example, will output a fault message.

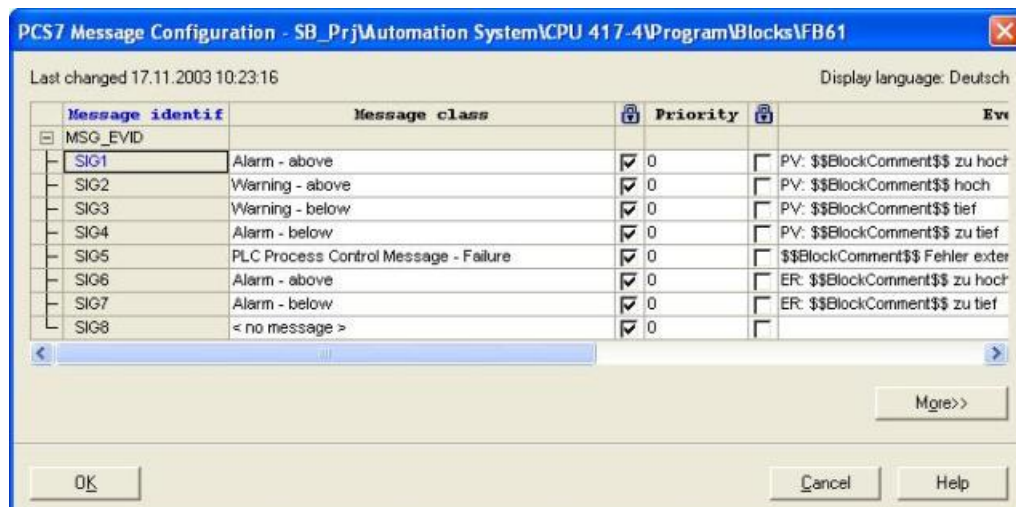
### 6.8.3 Priorities

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).



Reaktionszeit Response Time	Potenzielle Auswirkung / Seriousness		
	Anlagenstillstand Shutdown	Produktqualitätsverlust Off spec	Produktionsverzögerung Delay in production
< 5 min	Hoch High	Mittel Medium	Niedrig Low
	Mittel Medium	Niedrig Low	Niedrig Low
5 - 20 min	Mittel Medium	Niedrig Low	Niedrig Low
> 20 min	Niedrig Low	Niedrig Low	Niedrig Low
	Niedrig Low	Niedrig Low	Niedrig Low

The priority is defined on an instance-specific basis in PCS 7 during message configuration and is initially set to “0”.



It is preferable for the priorities to be set in the process object view.

## 6.8.4 Suppressing, Filtering, Hiding

### Suppressing Messages

In process mode, if he has the relevant rights 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, in the commissioning phase of a new process tag. 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 behavior 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, event-signaling 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 mimic diagram, 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:

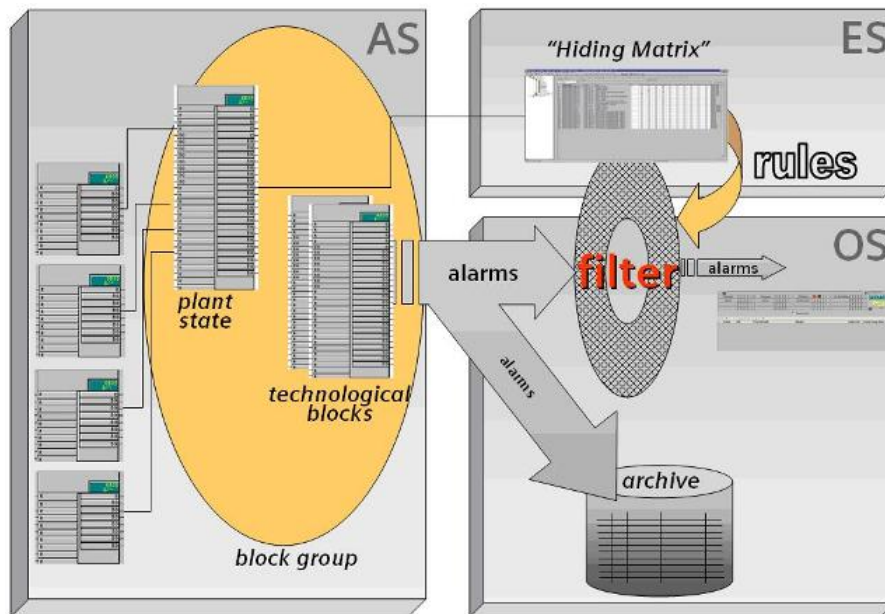
- Alarms hidden and shown manually
- Alarms hidden and shown automatically, depending on process states

#### Hiding alarms manually:

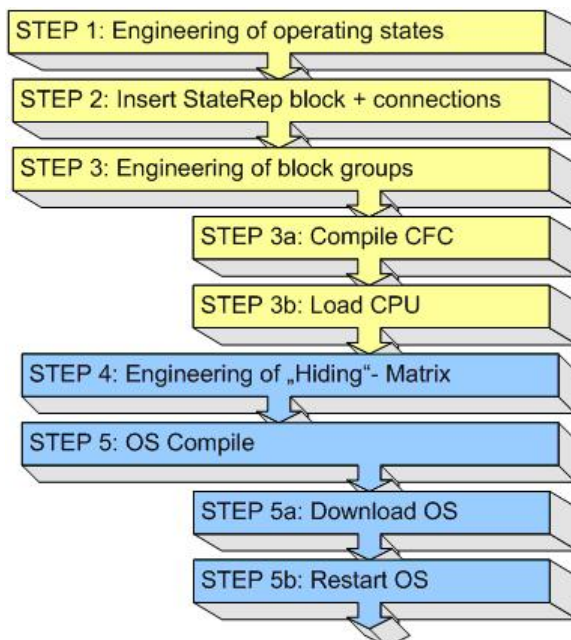
- The alarms are unhidden once a defined period of time has elapsed.
- Manually hidden alarms are acknowledged automatically.
- Manual alarm hiding applies to all clients of the relevant OS server.
- An operating message is output if alarms are hidden and shown manually.

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 (signaling) blocks are assigned to a status block via the new “block group” block property.



The system documentation describes the individual configuration steps for the illustration below in more detail.

**Note**

The major difference between message suppression and alarm hiding is that suppressed messages are not sent to the OS; by contrast, alarm hiding affects the alarm display only.

### 6.8.5 Monitoring PCS 7 Components

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 have been configured in HW Config and the OPC connections to the operator stations must have been created.

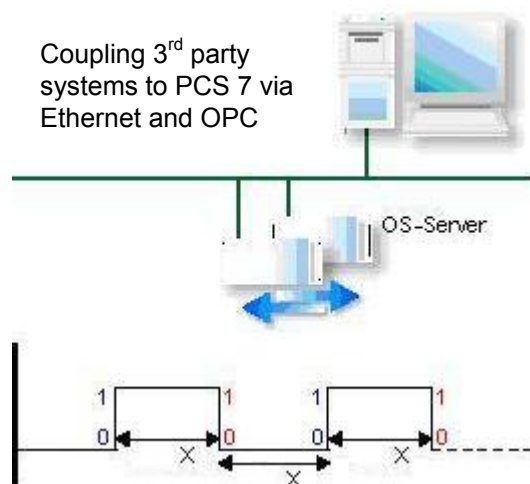
The nodes to be monitored are configured in the WinCC Explorer with the menu command **Editor > Lifebeat Monitoring > Open**. Here, all the nodes to be monitored and the monitoring cycle in which lifebeat monitoring is to take place can be set up.

Lifebeat Monitoring is activated automatically when the OS starts up.

Alternatively, all process control equipment can also be managed using PCS 7 Asset Management. A maintenance station (MS) can be used to provide an overview of the diagnostic and service information relating to all equipment. Asset Management does not require any additional configuration work. The configuration data is generated from the hardware and software configuration data.

### 6.8.6 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.

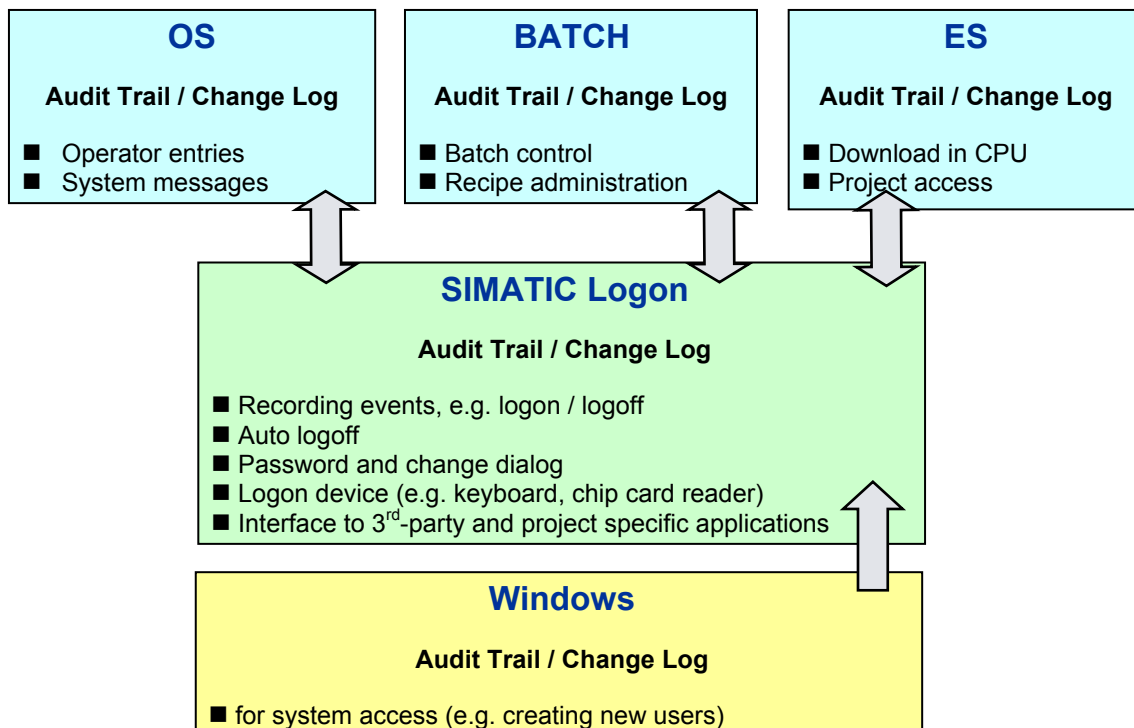
This procedure is repeated cyclically. If the connected system does not bring about a state change within the specified time, a process control message is generated in the SIMATIC PCS 7 process control system. This message indicates to the operator that communication with the connected system is not functioning correctly.

## 6.9 Audit Trail and Change Control

Operator inputs and critical changes to parameters and data must be saved on a user-specific basis in order to guarantee traceability (audit trail). Requirements of this topic are defined by authorities and organizations, e.g. 21 CFR 11 of the FDA (US authority).

In a controlled environment, changes to the project configuration or to the user administration, for example, must also be carefully managed.

As a result, PCS 7 systems feature a multi-layer concept as regards the audit trail and change control range of topics.



### 6.9.1 PCS 7 ES

#### Audit Trail on PCS 7 ES

Typically, configuration data which is not directly subject to the extremely strict requirements of 21 CFR 11 is dealt with on the engineering level. Having said that, the system components concerned are usually critical ones, 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 often practical and a customer requirement for such interventions to only be performed on the input level and if the corresponding operator permission is available, with changes being logged in the central OS audit trail.





---

**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 only be made via the OS level or on the ES by means of a change request, see also FAQ 23967880, 23907200, etc. about read-back of parameters.

---

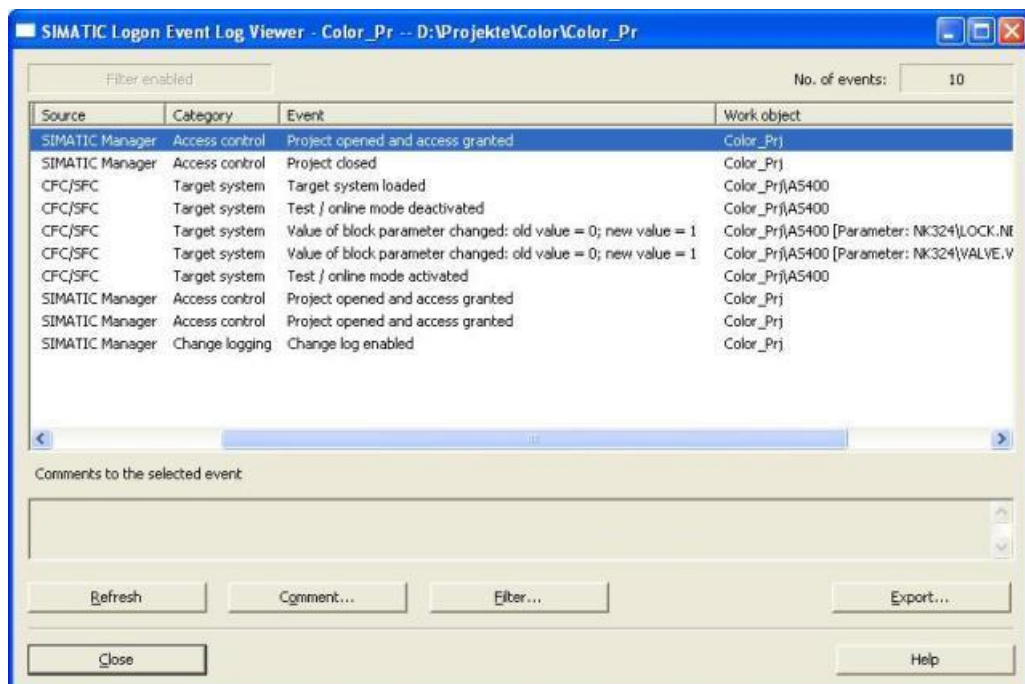
### **Change Control Regarding the ES Configuration and ES Project Engineering**

The Version Cross Manager is 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. This enables different project versions to be compared against one another, see chapter 7.4.2.

The current status of the offline/online configuration can also be verified by activating “test mode” in the ES. Parameter read back also has to be taken into account here, see “Note” in previous section.

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)



## Change Control Regarding AS Download

In addition to the ES configuration being protected against unauthorized access via the "Activate Access Protection" project setting, a CPU password can also be used to protect against unauthorized downloads being made 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 6.9.1 about 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 has been set up, the additional CPU password can often be done away with, if the customer agrees to it.

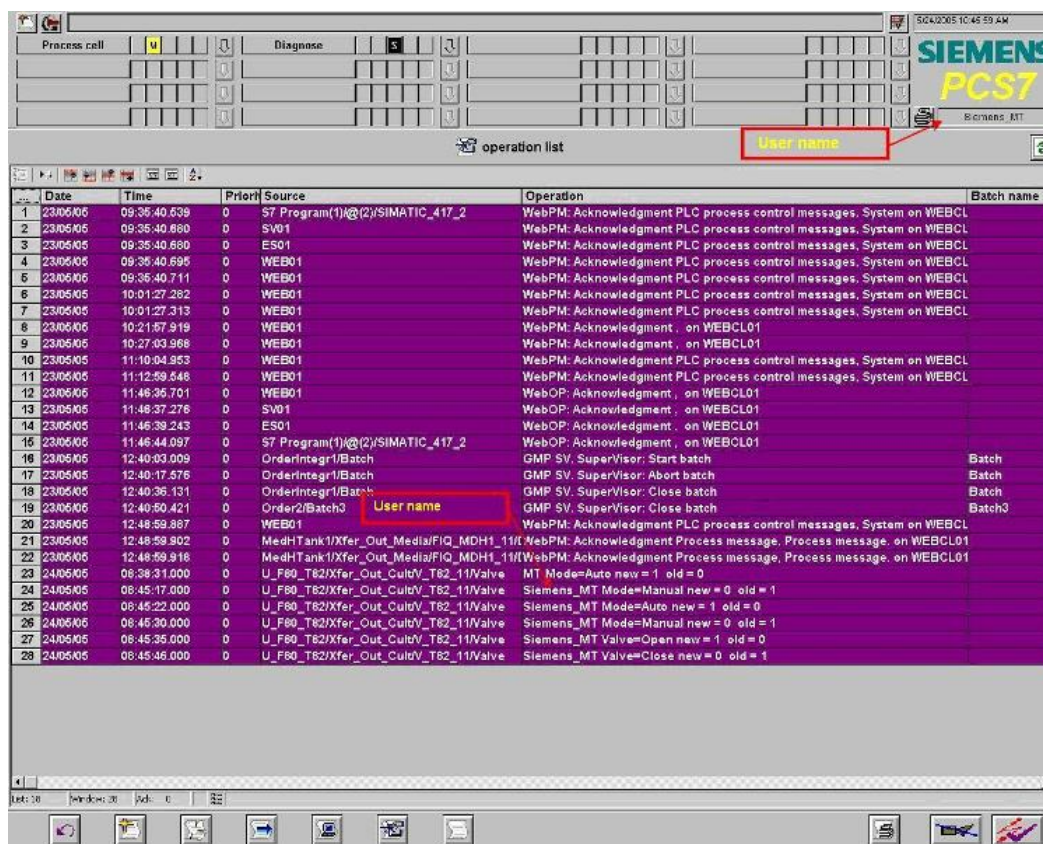
## 6.9.2 PCS 7 OS

### 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” event-signaling class in the message archive.

Acknowledgments of alarms, warnings, system messages, etc. are available in the chronicle of the process control system.

The figure below shows an extract taken from the operator input list. In row 24, an example parameter change is illustrated. The operator “Siemens MT” changed the mode from 1 to 0. The user ID of the user who is currently logged on can be seen in the overview area.



Date	Time	Priority	Source	Operation	Batch name
23/06/05	09:35:40.639	0	S7 Program(1)@2/SIMATIC_417_2	WebPM: Acknowledgment PLC process control messages, System on WEBCL	
23/06/05	09:35:40.680	0	SV01	WebPM: Acknowledgment PLC process control messages, System on WEBCL	
23/06/05	09:35:40.680	0	ES01	WebPM: Acknowledgment PLC process control messages, System on WEBCL	
23/06/05	09:35:40.695	0	WEB01	WebPM: Acknowledgment PLC process control messages, System on WEBCL	
23/06/05	09:35:40.711	0	WEB01	WebPM: Acknowledgment PLC process control messages, System on WEBCL	
23/06/05	10:01:27.282	0	WEB01	WebPM: Acknowledgment PLC process control messages, System on WEBCL	
23/06/05	10:01:27.313	0	WEB01	WebPM: Acknowledgment PLC process control messages, System on WEBCL	
23/06/05	10:21:57.919	0	WEB01	WebPM: Acknowledgment, on WEBCL01	
23/06/05	10:27:03.988	0	WEB01	WebPM: Acknowledgment, on WEBCL01	
23/06/05	11:10:04.953	0	WEB01	WebPM: Acknowledgment PLC process control messages, System on WEBCL	
23/06/05	11:12:59.548	0	WEB01	WebPM: Acknowledgment PLC process control messages, System on WEBCL	
23/06/05	11:46:36.701	0	WEB01	WebOP: Acknowledgment, on WEBCL01	
23/06/05	11:46:37.276	0	SV01	WebOP: Acknowledgment, on WEBCL01	
23/06/05	11:46:39.243	0	ES01	WebOP: Acknowledgment, on WEBCL01	
23/06/05	11:46:44.097	0	S7 Program(1)@2/SIMATIC_417_2	WebOP: Acknowledgment, on WEBCL01	
23/06/05	12:40:03.009	0	OrderIntegr1/Batch	GMP SV, SuperVisor: Start batch	Batch
23/06/05	12:40:17.576	0	OrderIntegr1/Batch	GMP SV, SuperVisor: Abort batch	Batch
23/06/05	12:40:36.131	0	OrderIntegr1/Batch	GMP SV, SuperVisor: Close batch	Batch
23/06/05	12:40:50.421	0	Order2/Batch3	GMP SV, SuperVisor: Close batch	Batch3
23/06/05	12:48:59.887	0	WEB01	WebPM: Acknowledgment PLC process control messages, System on WEBCL	
23/06/05	12:48:59.902	0	MedHTank1/Xfer_Out_Media/FIQ_MDH1_11	WebPM: Acknowledgment Process message, Process message, on WEBCL01	
23/06/05	12:48:59.918	0	MedHTank1/Xfer_Out_Media/FIQ_MDH1_11	WebPM: Acknowledgment Process message, Process message, on WEBCL01	
24/06/05	08:38:31.000	0	U_F80_T62/Xfer_Out_CultV_T62_11/Valve	MT Mode=Auto new = 1 old = 0	
24/06/05	08:45:17.000	0	U_F80_T62/Xfer_Out_CultV_T62_11/Valve	Siemens_MT Mode=Manual new = 0 old = 1	
24/06/05	08:45:22.000	0	U_F80_T62/Xfer_Out_CultV_T62_11/Valve	Siemens_MT Mode=Auto new = 1 old = 0	
24/06/05	08:45:30.000	0	U_F80_T62/Xfer_Out_CultV_T62_11/Valve	Siemens_MT Mode=Manual new = 0 old = 1	
24/06/05	08:45:36.000	0	U_F80_T62/Xfer_Out_CultV_T62_11/Valve	Siemens_MT Valve=Open new = 1 old = 0	
24/06/05	08:45:46.000	0	U_F80_T62/Xfer_Out_CultV_T62_11/Valve	Siemens_MT Valve=Close new = 0 old = 1	



#### Note

If parameter changes are made via input/output fields, message output must be configured separately.

#### Note

Select the hard disk capacity so that the entire audit trail can be stored there until it is transferred to an external data medium.

## Change Control Regarding the OS Configuration and OS Project Engineering

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. Changes made to individual OS elements must be controlled in accordance with the applicable change procedure following their initial release.

### 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).

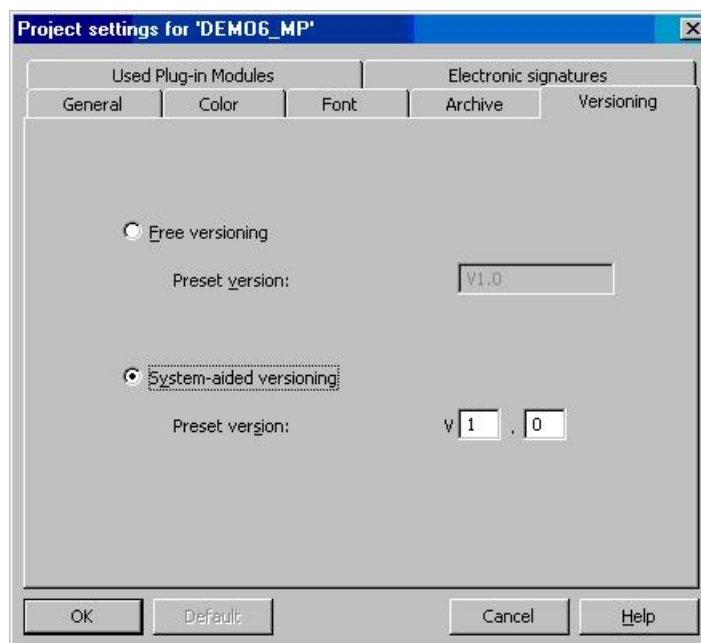
A batch report, in which information on the operations performed for each batch is logged (who, when, what), is also created in SIMATIC BATCH.

#### Change Control Regarding Recipes and Batch Objects

Changes made to recipe data and batch data (deleted batches, for example) are logged in the change log. The user, time, and action are entered in this log.

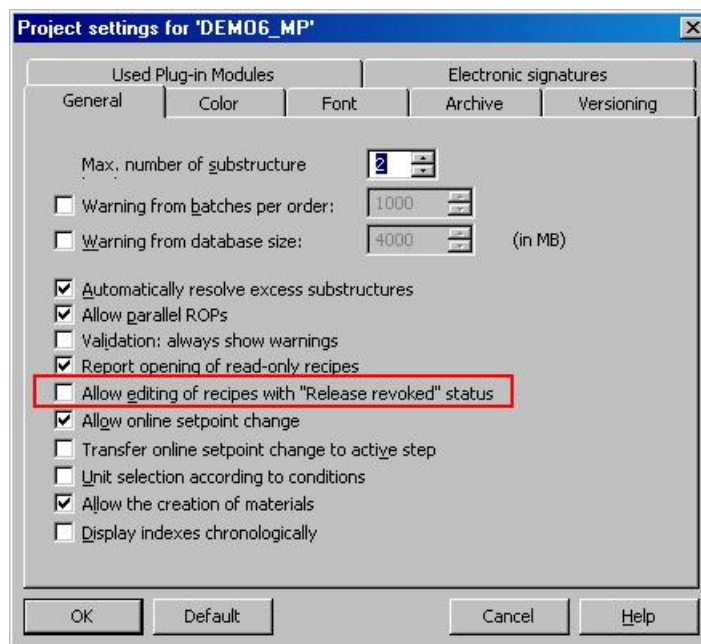
To ensure consistent version management, the following project settings must be made:

- “System-aided versioning” option selected



as well as

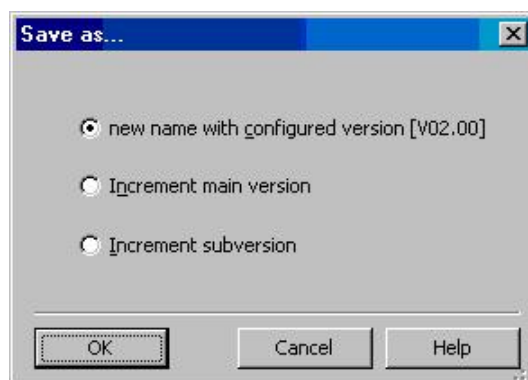
- **Allow editing of recipes in the “Release revoked” status** property deactivated



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



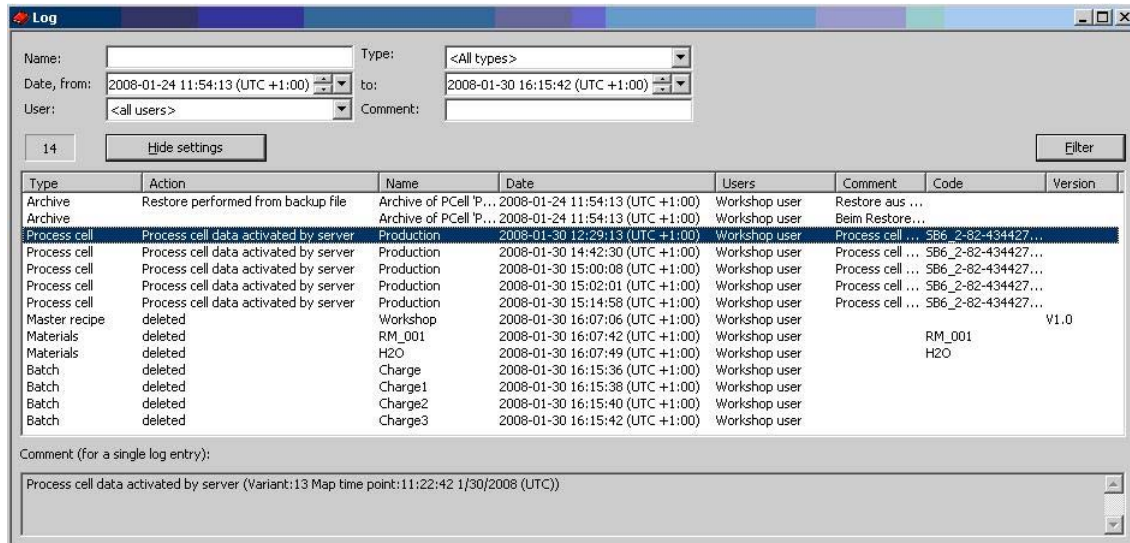
The recipe can only be edited after “Save As” has been used. The following prompt is displayed:



#### Note

If a new recipe based on a recipe which has already been released is to be created using “Save As”, the new recipe must first be generated using the “Save As” function **before any change is made to the existing recipe**. (FAQ 23378328) This ensures that, once released, a recipe cannot be subsequently edited without changing its version or name.

If recipes are deleted, this is recorded in the log; see figure below.





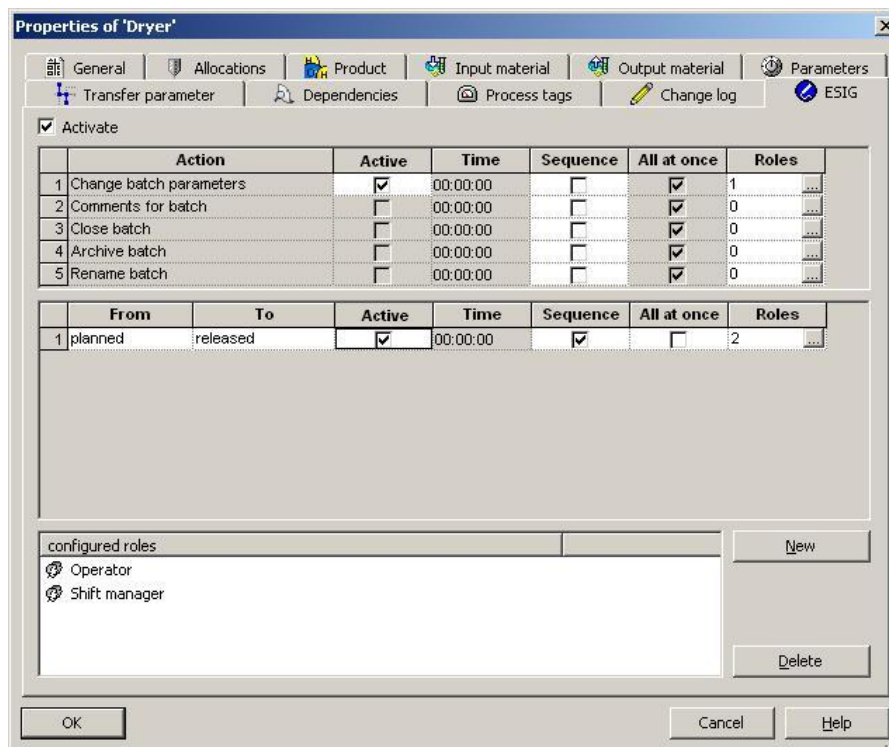
## 6.10 Configuration for Electronic Signatures

If electronic signatures are to be used within a computer system in lieu of handwritten signatures, certain legal regulations, such as those contained in 21 CFR 11 of the FDA (US authority), must be complied with.

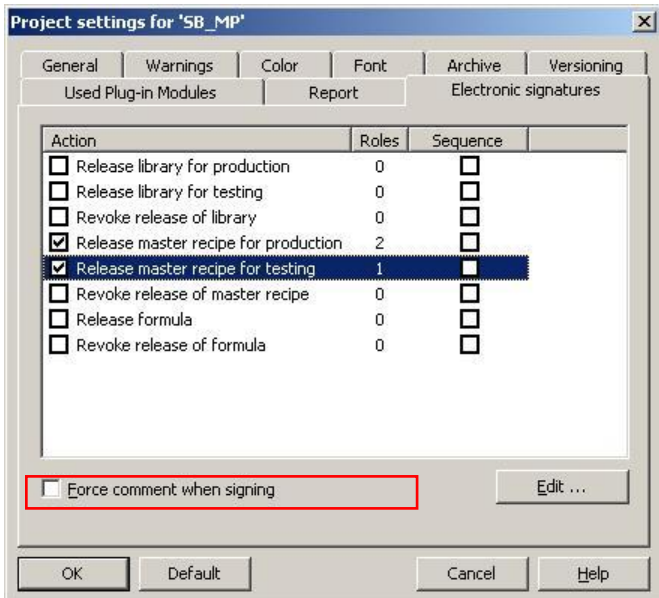
The locations where signatures are required are partly defined by other laws and regulations and partly by customer-specific demands. The process owner is always the one who decides which of these signatures are to be supplied electronically.

### 6.10.1 Electronic Signatures in SIMATIC BATCH

If SIMATIC Logon is installed, 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 a configuration dialog for setting up electronic signatures. Two electronic signatures are required in this example; they are specified in the SIMATIC BATCH Recipe Editor in the “configured roles” box.

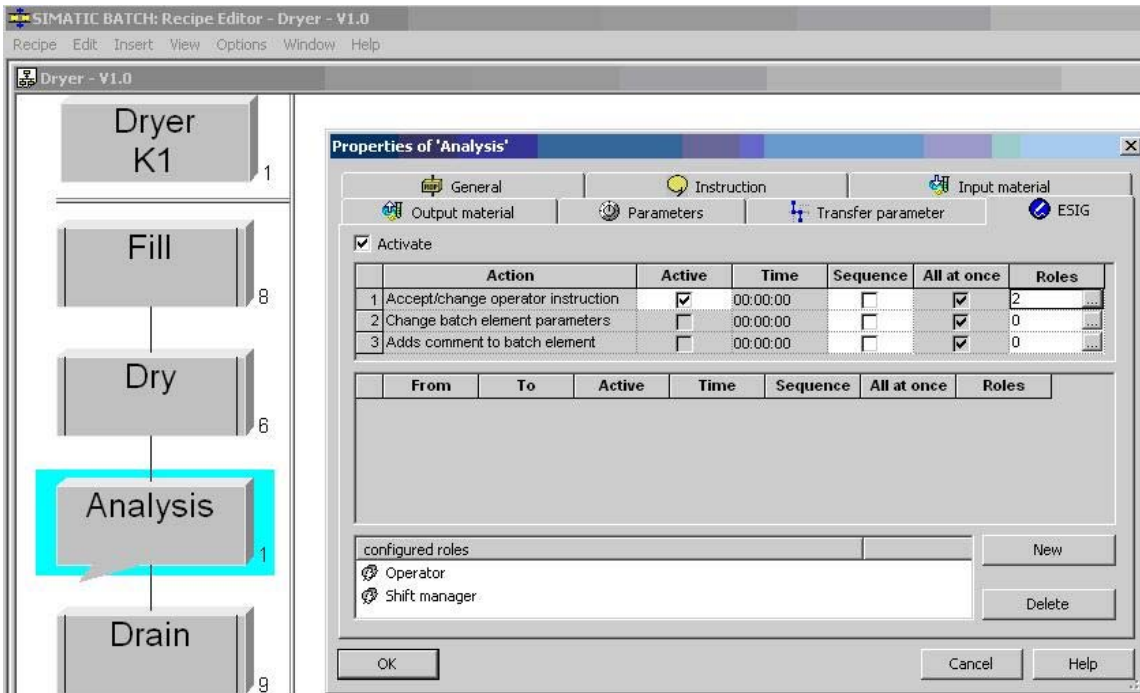


The project settings can also be used to make an electronic signature necessary for releasing recipes, parameter sets (formulas), and recipe operations, for example.



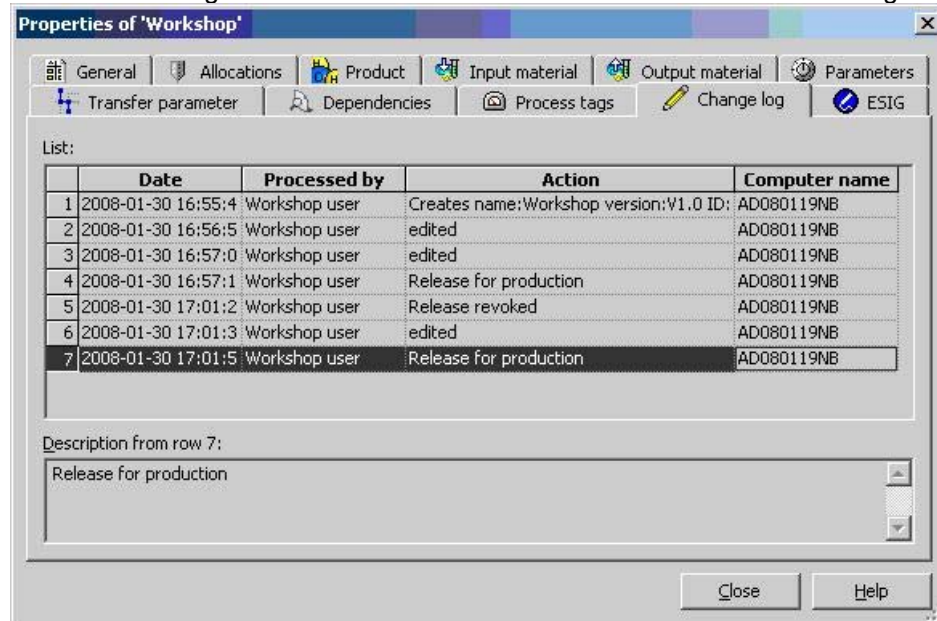
A comment can also be entered for each electronic signature; this comment can be forced in the mask shown above.

As well as these project-wide 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.





The electronic signatures created are stored in the SIMATIC BATCH change log.



### 6.10.2 Electronic Signatures on PCS 7 OS

See information in **GMP Engineering Manual WinCC V6.2**, section 6.4, about “Electronic Signature” as well as FAQ 24458155 and 27780448.

### 6.10.3 Electronic Signatures on PCS 7 ES

Configuration data in the engineering system is subject to change control and it must be possible to trace any changes made. The requirements of 21 CFR Part 11 as regards 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 should only be entered via the input level (OS) and, if required, assigned an electronic signature at that same location.

## 6.11 Data Backup

Backup copies of the configuration data must be made at regular intervals during the configuration phase; this ensures that the configuration data which has been created can be accessed again, for example after a hardware or hard disk failure.

It is also advisable to make a backup of the system partition containing the operating system, SIMATIC PCS 7 process control system software, etc.

---

**Note**

The backup of the application software and the backup of the system partition with and without SIMATIC PCS 7 should be stored on external media (for example, MOD, CD, DVD, network backup).

---

### 6.11.1 Backing Up the System Configuration

The operating system and the PCS 7 installation should be backed up as hard disk images. Such images can be used to restore the PC to its original status relatively easily.

#### Which images are Advisable?

- Create an image of the operating system installation with all drivers and all settings relating to the network, user administration, etc. without SIMATIC PCS 7.
- Create an image of the installed PCs with SIMATIC PCS 7.
- Create an image of the installed PCs with SIMATIC PCS 7 including all projects.



---

**Note**

An image can only be copied back to a PC with identical hardware. For this reason, the hardware configuration of the PCs must be appropriately documented.

Images of individual partitions cannot be exchanged between PCs because various settings, for example in the registry, differ from PC to PC.

---

## 6.11.2 Backing Up the Application Software

### Backing Up Application Software in the Engineering System

It is advisable to back up project data at regular intervals during the configuration phase and when changes are made to released application software. The SIMATIC Manager "Archive Project" system function should be used for this purpose. If version-specific archiving is required, the "Version Trail" optional package should be used, see chapter 7.4.1.

---

#### 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

In addition to the project configuration in PCS 7, the application data in SIMATIC BATCH (libraries, master recipes, materials, user rights, etc.) must also be backed up. This backup is created from within the SIMATIC BATCH Control Center.

The backup data can be copied back again using the "Restore" command.

## 6.12 Recording and Archiving Data Electronically

Several steps have to be performed in order to record and archive data electronically:

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

### 6.12.1 Specifying the Data to be Archived

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

- Definition of the data to be archived, coming from different sources: process values, messages, batch data and batch reports, audit trail data, log files, etc.
- The respective recording cycles
- The respective retention period for the data, online and offline
- The respective archiving cycles for external archiving

In PCS 7 this data is saved in various archives:

- "Tag Logging Fast" process value archive
- "Tag Logging Slow" process value archive
- Message archive
- OS and batch reports

There are further parts in the system where 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 of Windows Computer Management (logon/logoff activities, account management, rights settings for the file system, etc. according to the corresponding configuration)

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

## 6.12.2 Setting Up Process Value Archives

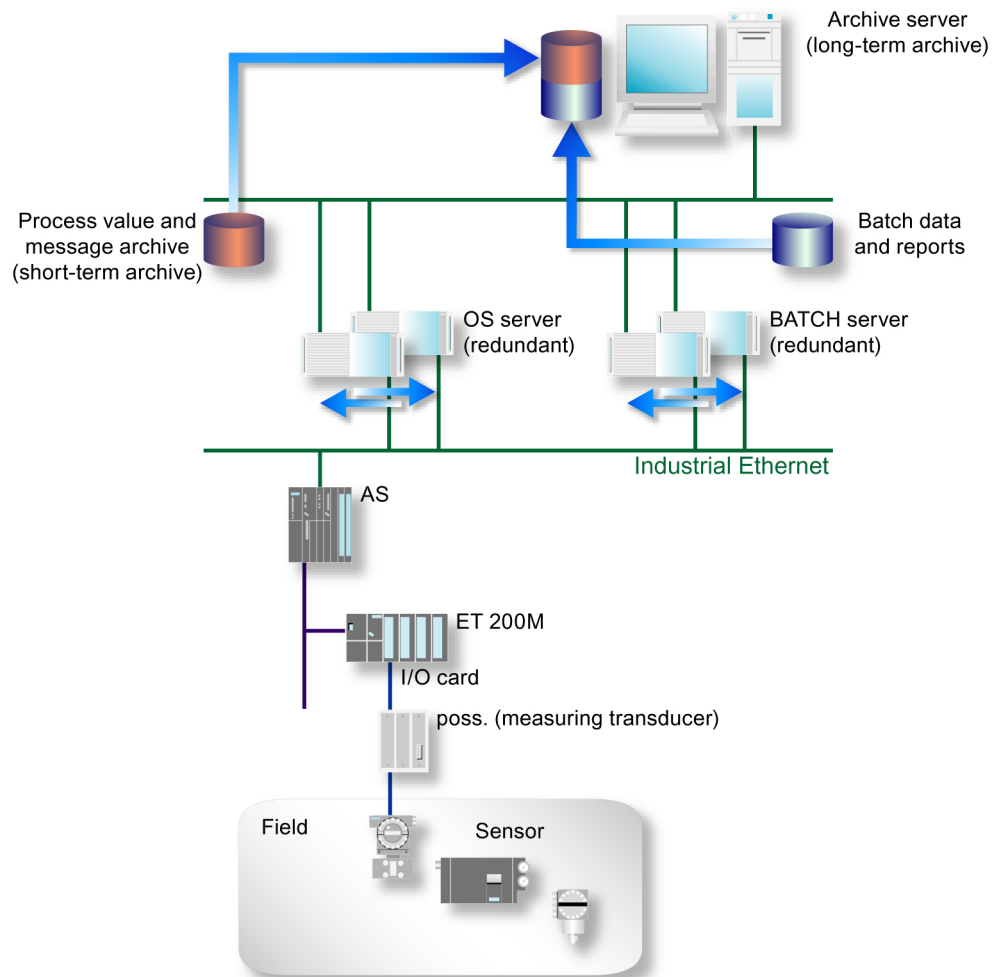
The procedure for configuring a process value archive is broken down into the following steps:

- 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 transferred out regularly at intervals which ensure that no data can be lost.



The process values and messages saved in the OS server can be transferred to the 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 (e.g. 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 (see graphic below).

Block	Block comment	I/O name	I/O comment	Pr...	OS	Archive name	Tag name	T...	Long-term a...	Tag supply	Archiving	Acquisition...	Factor for ar...	Archiving
1	PID Control	PV_IN	Process Val...		AD044289...	CTRL_TC311	REACT1/TC...		<input checked="" type="checkbox"/>	System	Released	500 ms	1	500 ms
2	PID Control	LMNR_IN	Feedb. of M...		AD044289...	CTRL_TC311	REACT1/TC...		<input checked="" type="checkbox"/>	System	Released	500 ms	1	500 ms
3	PID Control	SP	Active Setp...		AD044289...	CTRL_TC311	REACT1/TC...		<input checked="" type="checkbox"/>	System	Released	500 ms	1	500 ms
4	PID Control	PV_IN	Process Val...		AD044289...	FC111	RMT1/FC1...		<input checked="" type="checkbox"/>	System	Released	500 ms	1	500 ms
5	PID Control	LMNR_IN	Feedb. of M...		AD044289...	FC111	RMT1/FC1...		<input checked="" type="checkbox"/>	System	Released	500 ms	1	500 ms
6	PID Control	SP	Active Setp...		AD044289...	FC111	ColorRMT1...		<input checked="" type="checkbox"/>	System	Released	500 ms	1	500 ms
7	PID Control	SP	Active Setp...		AD044289...	FC111	RMT1/FC1...		<input checked="" type="checkbox"/>	System	Released	500 ms	1	500 ms

The specification documents (process tag list, Functional 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, when changing, etc.
- Cycle time
- Type of value (instantaneous value, mean value, maximum value, etc.)

Further information can be found in the manual **WinCC Basic Documentation**.

## 6.12.3 Long-Term Archiving with the Central Archive Server (CAS)

The CAS (Central Archive Server) is a standalone server PC, which does not require a connection to the plant bus. It is used for the long-term archiving of messages, process values, and reports.

Process values and messages which have been transferred out of the OS archives, as well as OS reports and batch data can be displayed either on the OS clients directly or by using the StoragePlus Viewer integrated in the CAS. The cycle for transferring data managed by the CAS can be configured, as can the associated segment size.

All clients which access archive data (short-term and long-term archives) must feature the server packages required by the server concerned, as well as the CAS server package.

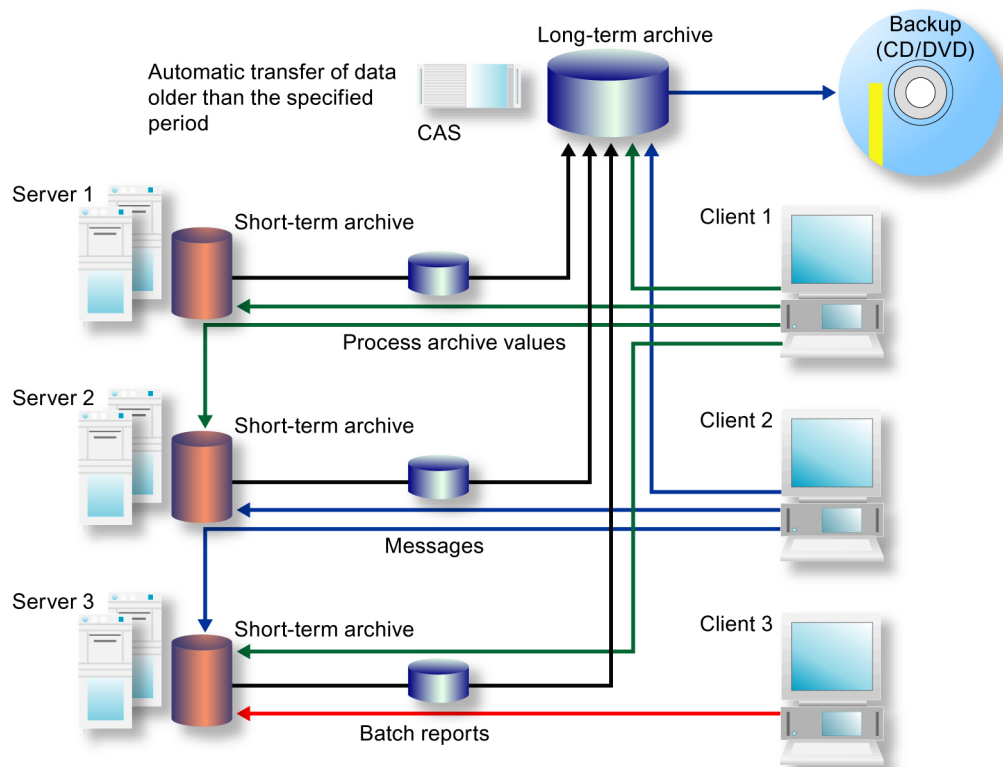
## Mode of Operation

Since the CAS is integrated in the PCS 7 system, process archive values can be clearly displayed on the OS clients in the form of trends and tables. To facilitate this, the CAS server data (package) must be stored on the OS clients when the system is configured or when a change is made to the system configuration.

Access to Tag Logging archive data for a defined time period is handled automatically within the system. This means that the user does not need to worry about whether selected archive data is still available on the OS servers or whether it has already been transferred to the CAS.

If the CAS has already transferred selected archive data to an external storage medium, with the result that the data is no longer “connected” to the CAS database (see section 6.12.2), these segments must be reconnected to the required time period. To achieve this, the segments are copied back to the CAS from the external storage medium.

The example shown in the figure below illustrates possible access options for displaying trends and tables (Tag Logging) on the OS clients.



## Installation

The database storage location (usually partition “D” on the hard disk) must be defined when the CAS component is installed.

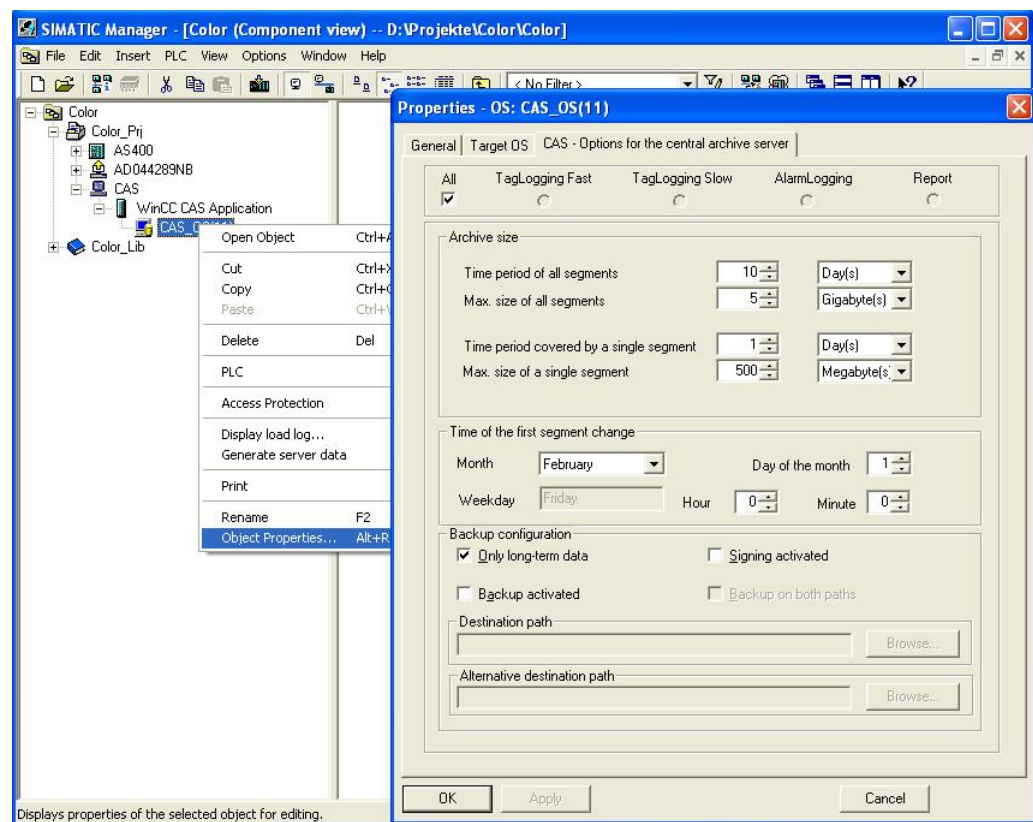
## Integration in the SIMATIC Manager

The CAS is centrally configured on the engineering station as described below.

A PC station must be created in HW Config and the "WinCC CAS Appl." HMI application added to it. If the CAS is to have a redundant structure, a second PC station must be configured with "WinCC CAS Appl. (stby)".

The archiving settings are made in the CAS "Properties" dialog. These settings can either be made collectively for all archive types or separately for each individual type.

Segment data remains available even after it has been copied to the specified backup location. The segment is only deleted if the associated "Time period for all segments" or "Max. size of all segments" parameter is exceeded.



Other activities relating to the destination paths, creation of server data (packages), start and execution of the Project Editor in the WinCC Explorer, and download to the CAS computer are essentially the same as for an OS server.

## Network Security

The central archive server requires access to the PCS 7 terminal bus to obtain data from the OS servers.

To this end, the CAS features a shared folder called "ArchivDir", to which the completed database segments of the OS servers are temporarily transferred.

If access from another network segment (Internet/Intranet) is required, please refer to the information contained in the manual titled **SIMATIC PCS 7 Security concept PCS 7 and WinCC**.



## Integration in Lifebeat Monitoring

Running the Project Editor also generates standard process control messages for the CAS, which can be viewed by all OS clients via the message display.

The CAS is integrated in Lifebeat Monitoring in the same way as SIMATIC PCS 7 components, as described in chapter 6.8.5. An OPC connection to the CAS simply needs to be set up, via which lifebeat monitoring can be performed.

## Visualizing CAS Data

Archived process values can be displayed on OS clients in the form of trends or tables.

In order to visualize messages, the integrated “StoragePlus Viewer” software package is used to define views of CAS databases. The data made available in this way is published using the Internet Information Server and can be viewed over an Intranet.

## Audit Trail

It is not technically possible to modify the data archived by the CAS, as the StoragePlus Viewer only provides users with read access to the archived data. This means that the CAS does not support an audit trail in the sense of 21 CFR Part 11. All events, such as the transfer of data to external media or failed transfers, are nevertheless saved in the log file folder of the CAS.

## Archiving

Process data is initially archived locally in single segments on the PCS 7 OS servers in Tag Logging or Alarm Logging. Once a single segment is completed, it is copied to the CAS. If the CAS has a redundant configuration, the single segment is copied to both computers.

---

### Note

The period for single segments on the OS servers in Tag Logging must be configured to be significantly shorter than the period for single segments of the CAS.

More information on configuration and archiving can be found in the relevant section of the engineering manual titled **PCS 7 V7.0 Operator Station**.

---

## 6.12.4 Long-Term Archiving With StoragePlus

StoragePlus consists of three software components:

- The **administrator console** (server application) allows the user to assign rights. Database settings and backups are also configured here. Access should be restricted to an authorized group of people.
- The **View Editor** is used to configure trends, message displays, and batch reports, which are saved in a separate view.
- The **Web Viewer** is used to display views created with the View Editor and published for this display.

### Mode of Operation

StoragePlus collects completed archive data segments from the servers together in a separate database according to chronological criteria so that they can be transferred on CD or DVD when a certain user-defined size is reached.

The database segments that result from the StoragePlus archiving procedure have the status "connected", which changes to "disconnected" when they are transferred. For StoragePlus to display archive values, the database segments must be "connected".

Archive data that has already been transferred can be "connected" to the StoragePlus database again. The "Catalog" call integrated in the administrator console in StoragePlus provides an overview of the current status of the database segments.

### Installation

StoragePlus is based on the MS SQL Server.

The installation instructions include detailed information on the installation order which must be followed and on the selection of partitions.

### Access Protection

The following default user groups exist in the StoragePlus administrator console:

- Administrator – full access to the StoragePlus system
- Power user – can read and create StoragePlus views
- User – can read StoragePlus views
- Guest – has no rights, neither access to StoragePlus views nor to the StoragePlus system

It is advisable to assign each user to just one group.

StoragePlus receives archive data and reports from the OS/BATCH servers via the PCS 7 terminal bus. A shared folder called "ArchivDir" is provided for this purpose, where this data is stored by means of file transfer.

The user who creates a view also has further editing rights for that view. This right can also be assigned to other users by means of the administrator console.

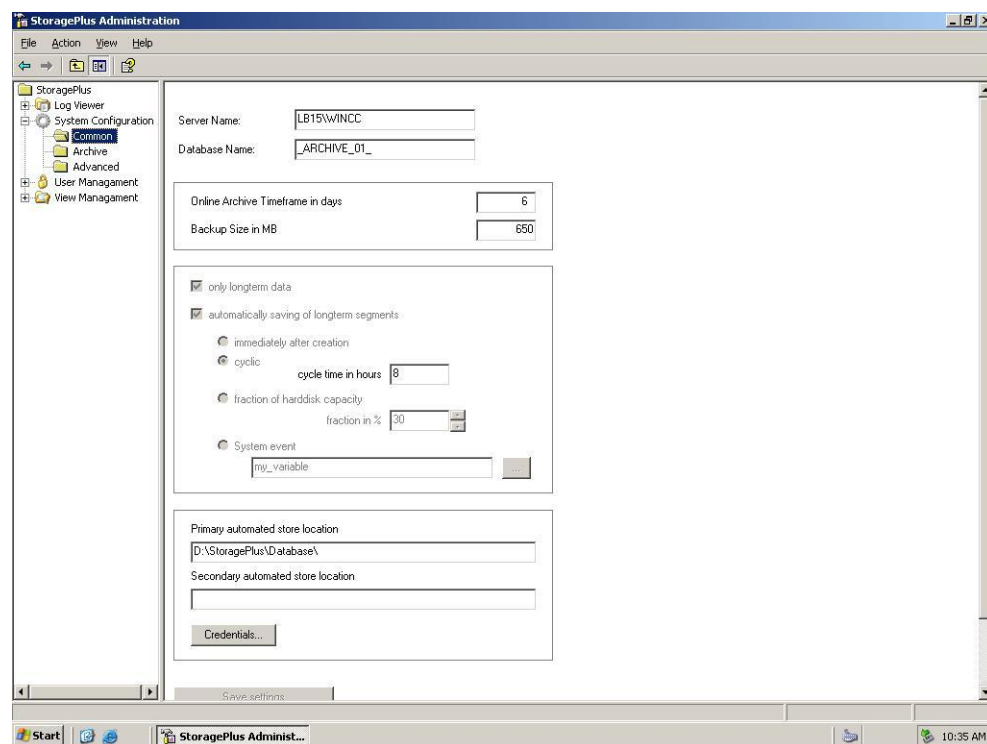
If he is not already logged on to the Windows operating system, the user can log on to the Web Viewer itself instead.

### Audit Trail

It is not technically possible to modify data archived in StoragePlus, as the StoragePlus Viewer only provides users with read access to the archived data. This means that StoragePlus does not support an audit trail in the sense of 21 CFR Part 11. User activities performed in the View Editor and StoragePlus application events are nevertheless recorded in log files.

- Application log presents the events to be recorded when archives are connected/disconnected, for example.
- Activity log contains events, such as changes to the configuration or the publication of views.

### Database Configuration



In PCS 7 it is possible to add an archiving identifier at the signal source in the CFC chart or in the process object view of the SIMATIC Manager:

- No archiving
- Archiving (short-term, storage on OS)
- Long-term archiving (storage on StoragePlus archive computer)

If this setting is missing, all the Tag Logging data archived and transferred by the OS servers is included.

### **Transferring Batch Reports from SIMATIC BATCH**

In order to integrate batch reports into StoragePlus long-term archiving, batch data must be transferred manually on completion of a batch. The default setting for this can be found in the SIMATIC BATCH Control Center (BCC) in:

“Options → Settings”, “Customize” dialog

The storage file type must be set to XML on the “Archive” tab. The storage location is once again the StoragePlus shared folder:

\\<targetcomputername>\ArchiveDir

### **Transferring Archive Data**

“Closed” database segments can be transferred manually or automatically. Once transferred, database segments receive the status “backuper & disconnected”. The transfer procedure may depend either on particular time periods or on the amount of free hard disk capacity available. It must be set up accordingly, taking the availability of data for online display (“connected” status) into account.

### **Backing Up Configuration Data**

StoragePlus maintains a table of contents of all database files which have been created, without which data that has already been transferred could not be accessed. This table of contents, along with the created views and other system settings, is needed in order to restore the system and must, therefore, be stored using the “Configuration Data” -> “Save” button.

---

#### **Recommendation**

This configuration data must be backed up regularly, for example, each time archive data is transferred.

---

## 6.13 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 agreed with the system user and specified accordingly. The following points must be considered in this regard:

- Power consumption of the systems to be supplied
- Power of the UPS
- Desired duration of UPS buffering

The power consumption of the systems to be buffered determines the size of the UPS. Another selection criterion is the priority of the systems. Systems with high priority are:

- Automation system (AS)
- Archive server
- Operator station (OS) server
- Operator station (OS) clients
- Network components

In any case, it is important to include the systems for logging data in the buffering procedure. The time at which the power failure occurred should also be recorded.

The use of UPS systems is accompanied by installation and configuration of software. The following must be taken into account:

- Configuration of power failure alarms
- Specification of the time to elapse before the PC is shut down
- Specification of the duration of UPS buffering

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.

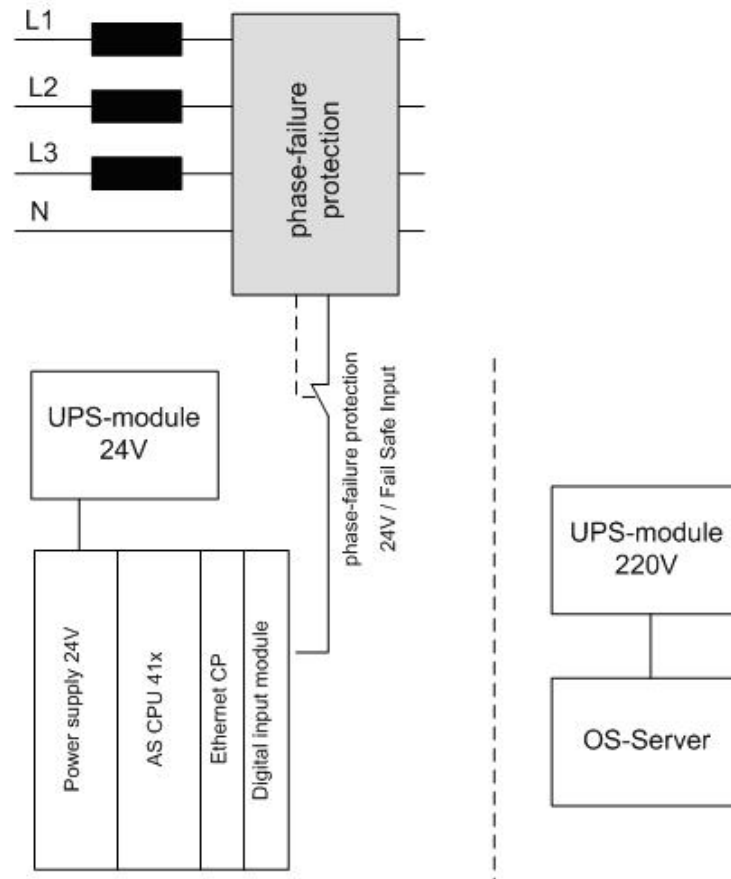
### 6.13.1 Configuring the UPS

The following table contains an example of the configuration of a UPS for an operator station in a process control system. The same basic procedure can be used with automation stations.

Case	Action	Reaction
1	Power failure < 10 seconds	The process control computers are buffered 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 computers are buffered by the UPS, for example, for 20 minutes. An alarm in the process control system documents the power failure and the shutdown of the process control computers after 20 minutes. The UPS stops supplying power after a defined time (for example, 25 minutes) so that an independent restart of the process control computers is possible once the power has been restored.
3	Power failure > 1 hour	The process control computers are buffered by the UPS, for example, for 20 minutes. An alarm in the process control system documents the power failure and the shutdown of the process control computers after 20 minutes. The UPS stops supplying power after a defined time so that an independent restart of the process control computers is possible once the power returns.

### 6.13.2 UPS Configuration over Digital Inputs

In addition to the standard backup provided by UPS devices, the option of monitoring the power supply should be used. This is done by monitoring the phase over one or more digital inputs, enabling power failures to be registered, signaled, and archived.



#### UPS Buffering 24 V

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 Buffering 220 V**

In addition to phase monitoring, the OS server is also buffered by standard UPS 220 V modules. This ensures that the server remains in operation 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 initiated by the operator or by 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 availability of the system when power returns.

### **6.13.3 MASTERGUARD UPS Systems**

All MASTERGUARD UPS systems belong to the “online UPS” category. They supply an output voltage free of interference voltage, electromagnetic interference, frequency variations, and voltage distortion. More detailed information on the different MASTERGUARD ranges can be found in the SIMATIC PCS 7 catalog.

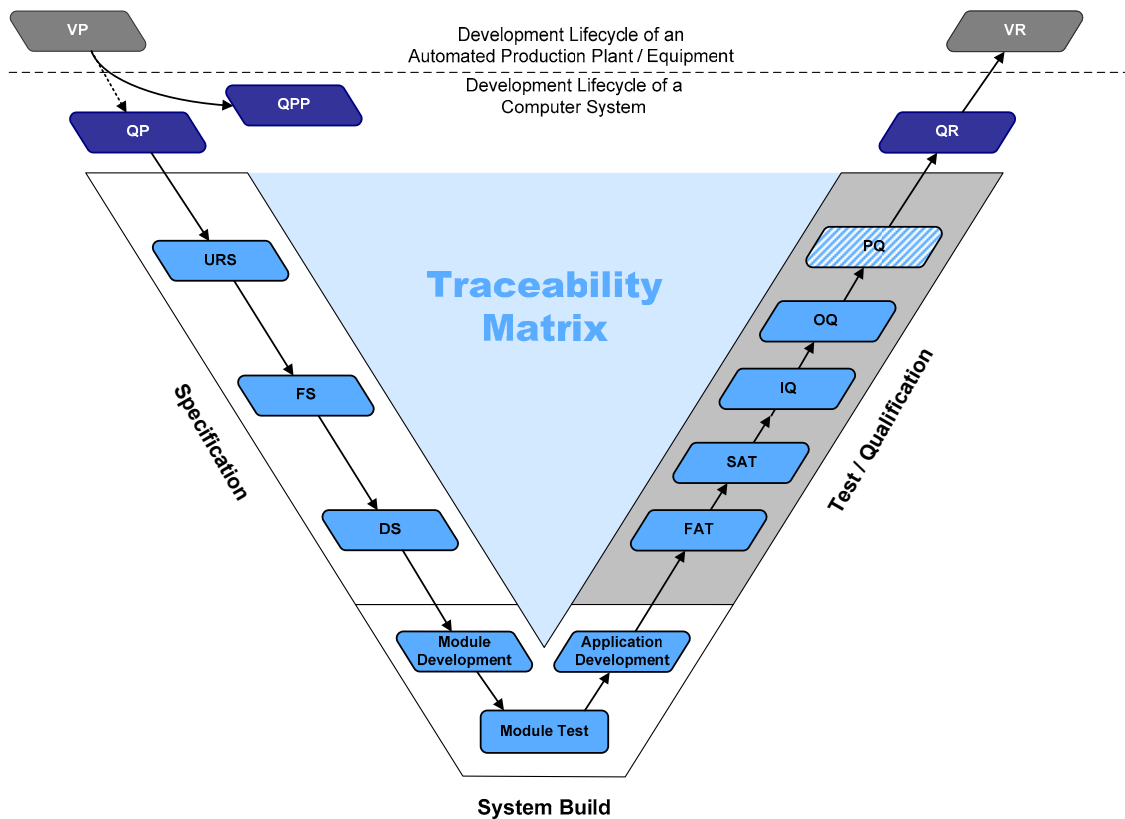




## 7 Support during Qualification

The aim of qualification is to provide documented evidence that the system was set up according to specifications (URS, FS, DS) and that all specified requirements have been met. The qualification describes, executes, and finally evaluates all the activities necessary for this. Various standard functionalities of SIMATIC PCS 7 can be used as support in qualification during IQ and OQ.

In the following graphic the highlighted area at the right-hand side illustrates the phase of the system qualification, where the activities of this section belong to.



## 7.1 Qualification Planning

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

The following are some of the issues defined at the outset of the project:

- Parties responsible for planning, performing and approval of tests
- Scope of tests in relation to the individual test phases
- Test environment (test equipment, 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 only very few tests need to be repeated, or even none at all.

---

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

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

## 7.2 Qualification of Hardware

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

---

### Note

Printouts and screenshots can be used to verify qualification (IQ/OQ) as appropriate.

A visual inspection of the hardware can be performed in addition.

---

### Qualification of Field Devices

Field devices are defined and qualified by means of the following information, for example:

- Manufacturer and type designation
- Order number
- Function / installation location
- Process tag name / measuring range / unit of measure

- Type of connection
- Address number

---

**Note**

SIMATIC PCS 7 Asset Management can offer support here.

---

## Qualification of the Automation Hardware

Automation stations are defined and qualified by means of the following information, for example:

- Manufacturer and type designation
- 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
- Etc.

---

**Note**

HW Config printouts support the relevant documentation.

The control cabinet documentation must comply with HW Config, too.

---

## Qualification of the Network Structure

The information below is an example of the data which could be defined and verified during qualification of the network structure:

- Name of station, PC, AS, clients, etc.
- Communication module, type of connection, and communication partner (Ethernet, PROFIBUS, serial, etc.)
- MAC address (when using the ISO protocol on the plant bus)
- TCP/IP address and subnet mask (when using clients)
- PROFIBUS addresses

---

**Note**

The SIMATIC NetPro configuration can be printed out.

---

## Specifying the PC Hardware Used

The information below is an example of the data which could be defined and verified during qualification 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

A PC pass contains detailed information on the configuration of the computer and can be printed out to verify qualification.

---

## 7.3 Qualification of Software

### 7.3.1 Software Categorization according to GAMP Guide

According to the *GAMP Guide* the software components of a system are assigned to one of five software categories for the purpose of validating automated systems. Concerning a PCS 7 system this means that the single software components cause different specification and test effort, according to their respective software category.

While a PCS 7-System as a whole would be classified as category 4 or sometimes even 5, the single standard components (without configuration) can be treated as a category 3 software, as far as specification and test efforts are concerned.

The configuration part based on installed products, libraries, function blocks, etc. matches the software category 4.

If, beyond this configuration, "free code" is written, this applies to category 5 software, meaning a much higher effort for specification and test of these software functions or packages.

### **7.3.2 Qualification of Standard Software**

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

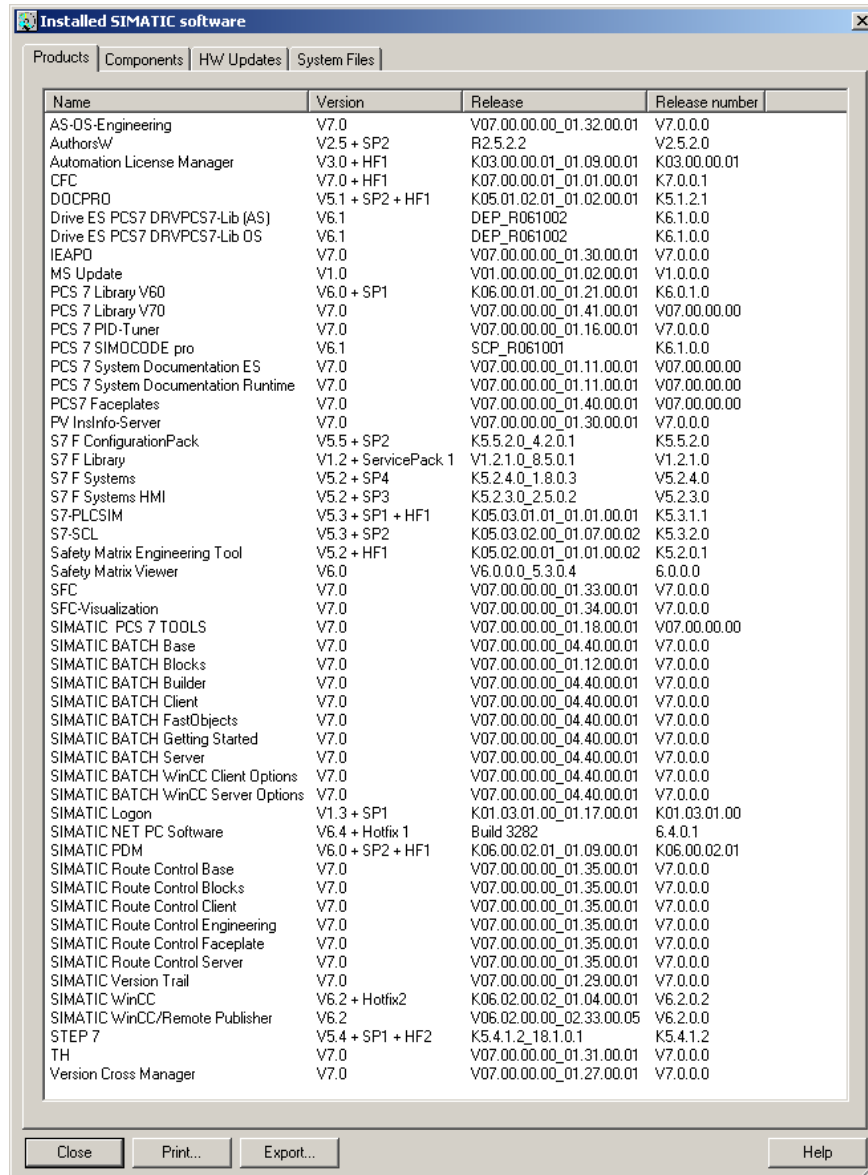
- Operating system and further software packages
- SIMATIC PCS 7 software packages (OS server, OS client, CAS, engineering system, BATCH server, BATCH client, etc.), SIMATIC IT server
- SIMATIC standard options (SIMATIC PDM, SIMATIC Logon, SFC Visualization, etc.)
- Standard libraries

#### **Operating System and further software packages**

The installed software can be verified by means of operating system functions. The information can be found under Control Panel > Add or Remove Programs. All installed software components are displayed here.

## SIMATIC Software

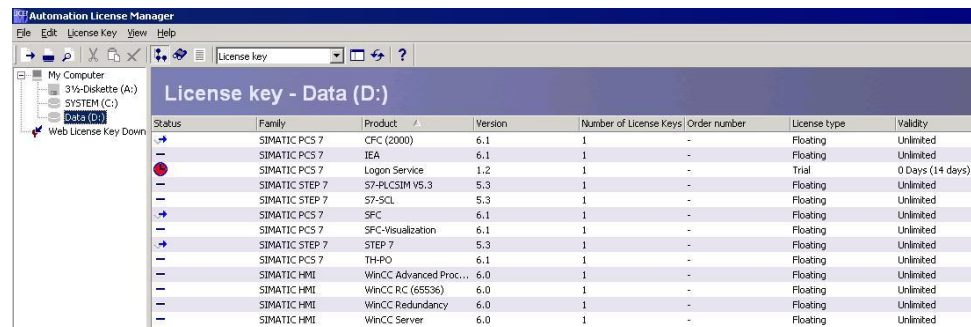
Installed SIMATIC software can be verified using the "Installed SIMATIC software" software tool. This tool provides information on the SIMATIC software currently installed on the computer.



Name	Version	Release	Release number
AS-OS-Engineering	V7.0	V07.00.00.01_32.00.01	V7.0.0.0
AuthorsW	V2.5 + SP2	R2.5.2.2	V2.5.2.0
Automation License Manager	V3.0 + HF1	K03.00.00.01_01.09.00.01	K03.00.00.01
CFC	V7.0 + HF1	K07.00.00.01_01.01.00.01	K7.0.0.1
DOCPRO	V5.1 + SP2 + HF1	K05.01.02.01_01.02.00.01	K5.1.2.1
Drive ES PCS7 DRVPCS7-Lib (AS)	V6.1	DEP_R061002	K6.1.0.0
Drive ES PCS7 DRVPCS7-Lib OS	V6.1	DEP_R061002	K6.1.0.0
IEAPO	V7.0	V07.00.00.01_30.00.01	V7.0.0.0
MS Update	V1.0	V01.00.00.00_01.02.00.01	V1.0.0.0
PCS 7 Library V60	V6.0 + SP1	K06.00.01.00_01.21.00.01	K6.0.1.0
PCS 7 Library V70	V7.0	V07.00.00.00_01.41.00.01	V07.00.00.00
PCS 7 PID-Tuner	V7.0	V07.00.00.00_01.16.00.01	V7.0.0.0
PCS 7 SIMOCODE pro	V6.1	SCP_R061001	K6.1.0.0
PCS 7 System Documentation ES	V7.0	V07.00.00.00_01.11.00.01	V07.00.00.00
PCS 7 System Documentation Runtime	V7.0	V07.00.00.00_01.11.00.01	V07.00.00.00
PCS7 Faceplates	V7.0	V07.00.00.00_01.40.00.01	V07.00.00.00
PV InsInfo-Server	V7.0	V07.00.00.00_01.30.00.01	V7.0.0.0
S7 F ConfigurationPack	V5.5 + SP2	K5.5.2.0_4.2.0.1	K5.5.2.0
S7 F Library	V1.2 + ServicePack 1	V1.2.1.0_8.5.0.1	V1.2.1.0
S7 F Systems	V5.2 + SP4	K5.2.4.0_1.8.0.3	V5.2.4.0
S7 F Systems HMI	V5.2 + SP3	K5.2.3.0_2.5.0.2	V5.2.3.0
S7-PLCSIM	V5.3 + SP1 + HF1	K05.03.01.01_01.01.00.01	K5.3.1.1
S7-SCL	V5.3 + SP2	K05.03.02.00_01.07.00.02	K5.3.2.0
Safety Matrix Engineering Tool	V5.2 + HF1	K05.02.00.01_01.01.00.02	K5.2.0.1
Safety Matrix Viewer	V6.0	V6.0.0.0_5.3.0.4	6.0.0.0
SFC	V7.0	V07.00.00.00_01.33.00.01	V7.0.0.0
SFC-Visualization	V7.0	V07.00.00.00_01.34.00.01	V7.0.0.0
SIMATIC PCS 7 TOOLS	V7.0	V07.00.00.00_01.18.00.01	V07.00.00.00
SIMATIC BATCH Base	V7.0	V07.00.00.00_04.40.00.01	V7.0.0.0
SIMATIC BATCH Blocks	V7.0	V07.00.00.00_01.12.00.01	V7.0.0.0
SIMATIC BATCH Builder	V7.0	V07.00.00.00_04.40.00.01	V7.0.0.0
SIMATIC BATCH Client	V7.0	V07.00.00.00_04.40.00.01	V7.0.0.0
SIMATIC BATCH FastObjects	V7.0	V07.00.00.00_04.40.00.01	V7.0.0.0
SIMATIC BATCH Getting Started	V7.0	V07.00.00.00_04.40.00.01	V7.0.0.0
SIMATIC BATCH Server	V7.0	V07.00.00.00_04.40.00.01	V7.0.0.0
SIMATIC BATCH WinCC Client Options	V7.0	V07.00.00.00_04.40.00.01	V7.0.0.0
SIMATIC BATCH WinCC Server Options	V7.0	V07.00.00.00_04.40.00.01	V7.0.0.0
SIMATIC Logon	V1.3 + SP1	K01.03.01.00_01.17.00.01	K01.03.01.00
SIMATIC NET PC Software	V6.4 + Hotfix 1	Build 3282	6.4.0.1
SIMATIC PDM	V6.0 + SP2 + HF1	K06.00.02.01_01.09.00.01	K06.00.02.01
SIMATIC Route Control Base	V7.0	V07.00.00.00_01.35.00.01	V7.0.0.0
SIMATIC Route Control Blocks	V7.0	V07.00.00.00_01.35.00.01	V7.0.0.0
SIMATIC Route Control Client	V7.0	V07.00.00.00_01.35.00.01	V7.0.0.0
SIMATIC Route Control Engineering	V7.0	V07.00.00.00_01.35.00.01	V7.0.0.0
SIMATIC Route Control Faceplate	V7.0	V07.00.00.00_01.35.00.01	V7.0.0.0
SIMATIC Route Control Server	V7.0	V07.00.00.00_01.35.00.01	V7.0.0.0
SIMATIC Version Trail	V7.0	V07.00.00.00_01.29.00.01	V7.0.0.0
SIMATIC WinCC	V6.2 + Hotfix2	K06.02.00.02_01.04.00.01	V6.2.0.2
SIMATIC WinCC/Remote Publisher	V6.2	V06.02.00.00_02.33.00.05	V6.2.0.0
STEP 7	V5.4 + SP1 + HF2	K5.4.1.2_18.1.0.1	K5.4.1.2
TH	V7.0	V07.00.00.00_01.31.00.01	V7.0.0.0
Version Cross Manager	V7.0	V07.00.00.00_01.27.00.01	V7.0.0.0

## Software Licenses

The “Automation License Manager” SIMATIC tool provides information on the licenses currently installed on the process control PC. To view this information, open the Automation License Manager and select the PC partition on which the licenses are installed on the left-hand side in the Explorer bar. All available system licenses are now shown on the right-hand side of the window.

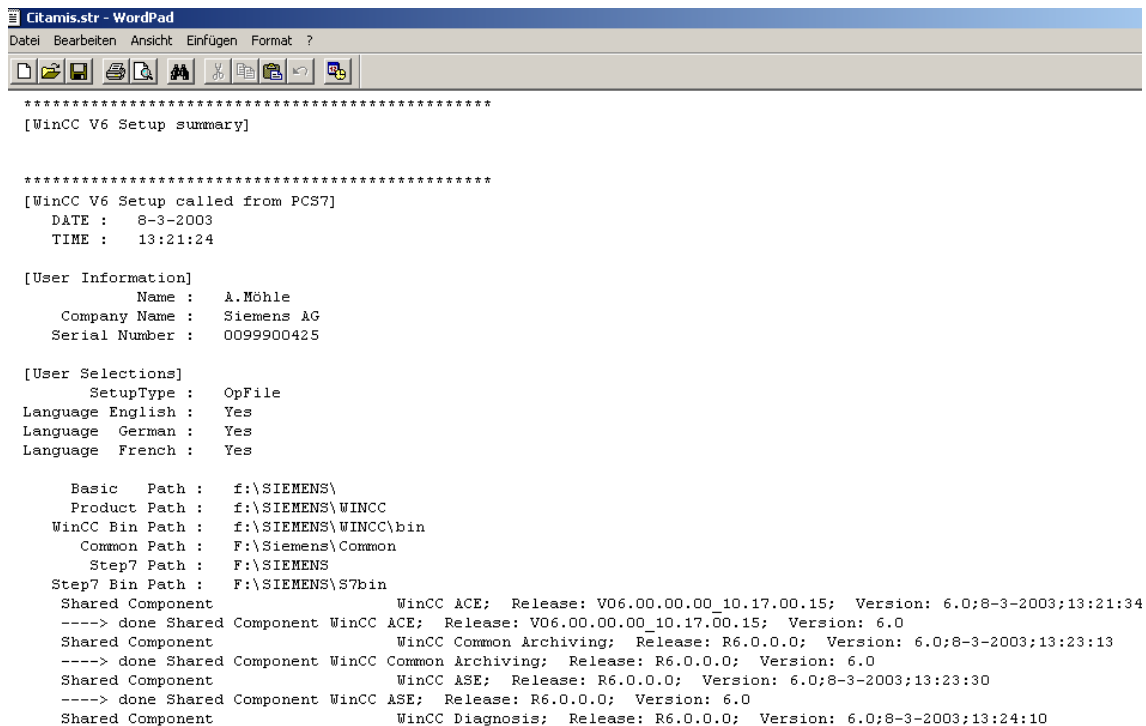


The screenshot shows the 'Automation License Manager' window. The left pane shows the file explorer with 'Data (D:)' selected. The right pane displays a table titled 'License key - Data (D:)' with the following columns: Status, Family, Product, Version, Number of License Keys, Order number, License type, and Validity.

Status	Family	Product	Version	Number of License Keys	Order number	License type	Validity
+	SIMATIC PCS 7	CFC (2000)	6.1	1	-	Floating	Unlimited
-	SIMATIC PCS 7	IEA	6.1	1	-	Floating	Unlimited
-	SIMATIC PCS 7	Logon Service	1.2	1	-	Trial	0 Days (14 days)
-	SIMATIC STEP 7	S7-PLCSIM V5.3	5.3	1	-	Floating	Unlimited
-	SIMATIC STEP 7	S7-SCL	5.3	1	-	Floating	Unlimited
+	SIMATIC PCS 7	SFC	6.1	1	-	Floating	Unlimited
-	SIMATIC PCS 7	SFC-Visualization	6.1	1	-	Floating	Unlimited
+	SIMATIC STEP 7	STEP 7	5.3	1	-	Floating	Unlimited
-	SIMATIC PCS 7	TH-PO	6.1	1	-	Floating	Unlimited
-	SIMATIC HMI	WinCC Advanced Proc...	6.0	1	-	Floating	Unlimited
-	SIMATIC HMI	WinCC RC (65536)	6.0	1	-	Floating	Unlimited
-	SIMATIC HMI	WinCC Redundancy	6.0	1	-	Floating	Unlimited
-	SIMATIC HMI	WinCC Server	6.0	1	-	Floating	Unlimited

## SIMATIC PCS 7

When SIMATIC PCS 7 is installed, the current status of the installed system programs is saved in the “citamis.str” file. Reinstallations are also documented. Depending on which operating system is installed, this file is located in either the “WINNT” or the “WINDOWS” folder.



The screenshot shows a WordPad window titled 'Citamis.str - WordPad'. The content of the file is as follows:

```

*****
[WinCC V6 Setup summary]

*****
[WinCC V6 Setup called from PCS7]
  DATE : 8-3-2003
  TIME : 13:21:24

[User Information]
  Name : A.Möhle
  Company Name : Siemens AG
  Serial Number : 0099900425

[User Selections]
  SetupType : OpFile
  Language English : Yes
  Language German : Yes
  Language French : Yes

  Basic Path : f:\SIEMENS\
  Product Path : f:\SIEMENS\WINCC
  WinCC Bin Path : f:\SIEMENS\WINCC\bin
  Common Path : F:\SIEMENS\Common
  Step7 Path : F:\SIEMENS
  Step7 Bin Path : F:\SIEMENS\S7bin
  Shared Component WinCC ACE; Release: V06.00.00.00_10.17.00.15; Version: 6.0;8-3-2003;13:21:34
----> done Shared Component WinCC ACE; Release: V06.00.00.00_10.17.00.15; Version: 6.0
  Shared Component WinCC Common Archiving; Release: R6.0.0.0; Version: 6.0;8-3-2003;13:23:13
----> done Shared Component WinCC Common Archiving; Release: R6.0.0.0; Version: 6.0
  Shared Component WinCC ASE; Release: R6.0.0.0; Version: 6.0;8-3-2003;13:23:30
----> done Shared Component WinCC ASE; Release: R6.0.0.0; Version: 6.0
  Shared Component WinCC Diagnosis; Release: R6.0.0.0; Version: 6.0;8-3-2003;13:24:10
  
```



### 7.3.3 Qualification of the Application Software

During qualification of the application software, checks are made to verify whether or not the created software meets the requirements of the specifications (FS/DS). Test descriptions (e.g. for FAT/SAT) must be agreed with the user and generated. These descriptions must take the complexity of the software and the design specifications into account.

The aspects listed below are typical elements of such tests, and can be used as a reference for the subsequent qualification steps:

- Checking the name of the application software
- Checking the plant hierarchy (process cell, unit, equipment module, single control element, etc.)
- Software module test (typical test)
- Checking communication with other nodes (third-party controllers, MES systems, etc.)
- Checking all inputs and outputs
- Checking all control modules (control-loop level)
- Checking all equipment phases and equipment operations (equipment phases)
- Checking the relationships between modes (MANUAL/AUTOMATIC switchovers, interlocks, start, running, held, aborting, completed, etc.)
- Checking process tag names
- Checking the visualization structure (P&I representation)
- Checking the operator input philosophy (access control, group rights, user rights)
- Checking archiving concepts (short-term archives, long-term archives)
- Checking the message concept
- Checking trends, graphs
- Checking time synchronization



#### Notice

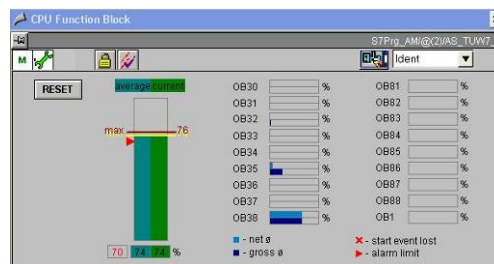
If other blocks are needed in addition to the PCS 7 standard libraries in order to configure specific processes or functions, the block libraries (FB, FC, DB) of the PCS 7 Add-On catalog should be used if possible.

If blocks created by the user are to be employed, significantly more work will be required in terms of specification, creation, and validation; this fact should be taken into consideration.

---

## Analyzing the CPU Load

Asset management can be used to analyze and document CPU utilization.



## DOCPRO

The licensed DOCPRO option is a user-friendly tool for creating a consistent plant log including versioning. All the data created with a configuration tool can be inserted in DOCPRO documentation. The data is therefore available in a clearly structured form and can be used centrally for qualification.

For further information see the system documentation as well as the **GMP Engineering Manual Step 7, chapter 4.4.3**.

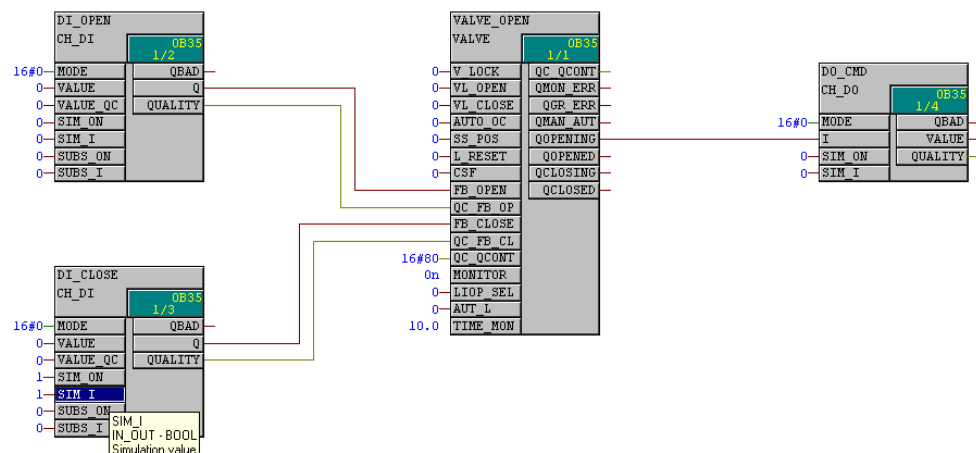
### 7.3.4 Simulation for Test Mode

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 configuration 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.

## Activating Simulation

Simulation for test purposes can be activated at the channel input or channel output driver blocks.

Using the example of a valve, simulation is activated at the SIM\_ON inputs and the input can be simulated at the SIM\_I input.



## Deactivating Simulation



---

### Notice

The activated simulations should be documented in accordance with good practice. A table provides an overview of all active simulations. On completion of the test phase, all simulations must be deactivated again.

---

---

### Recommendation

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 deactivated, thus switching simulation off from a central location.

---

## SIMIT Simulation Software

The SIMIT simulation software 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 not only simple signal tests at the touch of a button, but also complex function tests (such as temperature control).

Used in conjunction with the S7 PLCSIM PLC simulation software, which simulates 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 supplier in carrying out the Factory Acceptance Test (FAT), for example.

## 7.4 Configuration Control

### 7.4.1 Versioning Projects with “Version Trail”

SIMATIC PCS 7 Version Trail can be used to archive multiprojects, single projects, and project-specific libraries with a unique version ID. Archiving is executed in accordance with the PCS 7 archiving procedure. Project-specific libraries are backed up when a multiproject is archived, which means they remain assigned to the relevant multiproject.

SIMATIC PCS 7 Version Trail ensures continuous increment of the version according to validation factors. A completed version can no longer be changed. However, every archived version can be read back into the system.

As GMP requirements demand that SIMATIC Logon is used, all relevant actions are saved with details of the logged-on user.

---

### Note

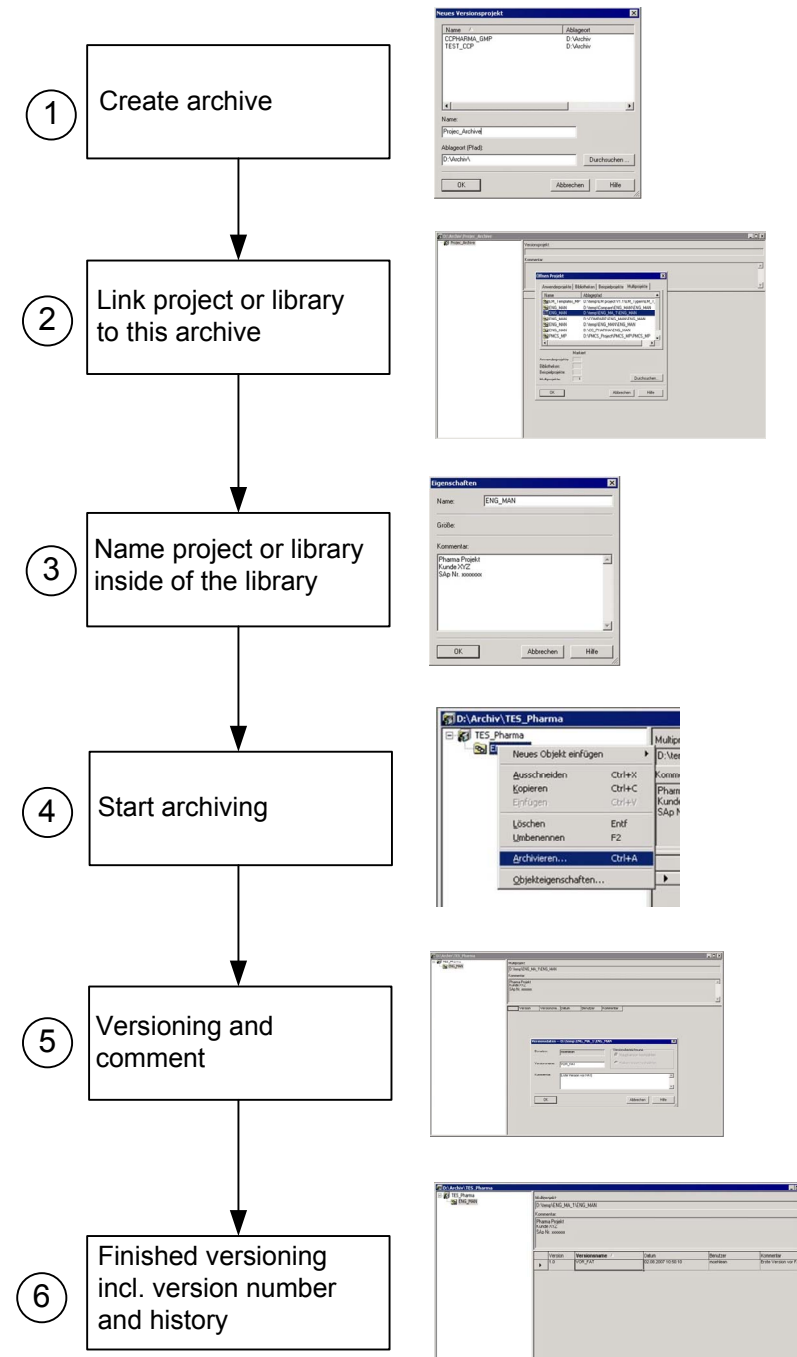
Before a multiproject is archived, a check must be performed to ensure that no projects or libraries belonging to the multiproject have been removed. This is because only projects and libraries contained in the multiproject at the time of archiving will actually be archived.

---

For further information see *online help* of SIMATIC PCS 7, topic “Version Trail”, as well as the engineering manual *PCS 7 Engineering System*.

## Procedure for Archiving Projects

The procedure described below explains how projects are versioned.



Several multiprojects, projects, and libraries can be assigned to one archive (repeat step 2-5). If a new project version is required, steps 4 and 5 must be repeated. SIMATIC PCS 7 Version Trail can be called via the Windows start menu or via the SIMATIC Manager.

Each archived project version can be retrieved in the SIMATIC Manager or by using Version Trail. In a validated plant, however, previous project versions can only be read back (retrieved) in exceptional cases and in consultation with the process owner (customer).



#### Note

The projects to be archived must not be opened in the SIMATIC Manager.

## 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 also chapter 7.4.2.

## 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 using the **Options > Version History** menu. All actions relating to the archiving of projects and deletion of versions are logged. The figure below shows an example version history, from the creation of versioned project "Sample1" through to the archiving of different versions.

Version History					
	Action	Name	Date	User	Comment
1	New versioned project	Version	01/30/2008 12:37:54 PM	Manuel	Versioned project created as 'D:\Archive\Version'.
2	New archive	\Color_Prj	01/30/2008 12:38:12 PM	Manuel	Project '\Color_Prj' pasted.
3	Archive version	\Color_Prj	01/30/2008 12:39:05 PM	Manuel	'\Color_Prj' Version '1.0' of 'D:\Projekte\Color\Color_Pr' archived.
4	New archive	\Color_Prj (2)	01/30/2008 12:48:16 PM	Manuel	Project '\Color_Prj (2)' pasted.
5	Archive version	\Color_Prj (2)	01/30/2008 12:49:43 PM	Manuel	'\Color_Prj (2)' Version '1.0' of 'D:\Projekte\Color\Color_Pr' archived.

Close    Print...    Print Preview    Help

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 life cycle.

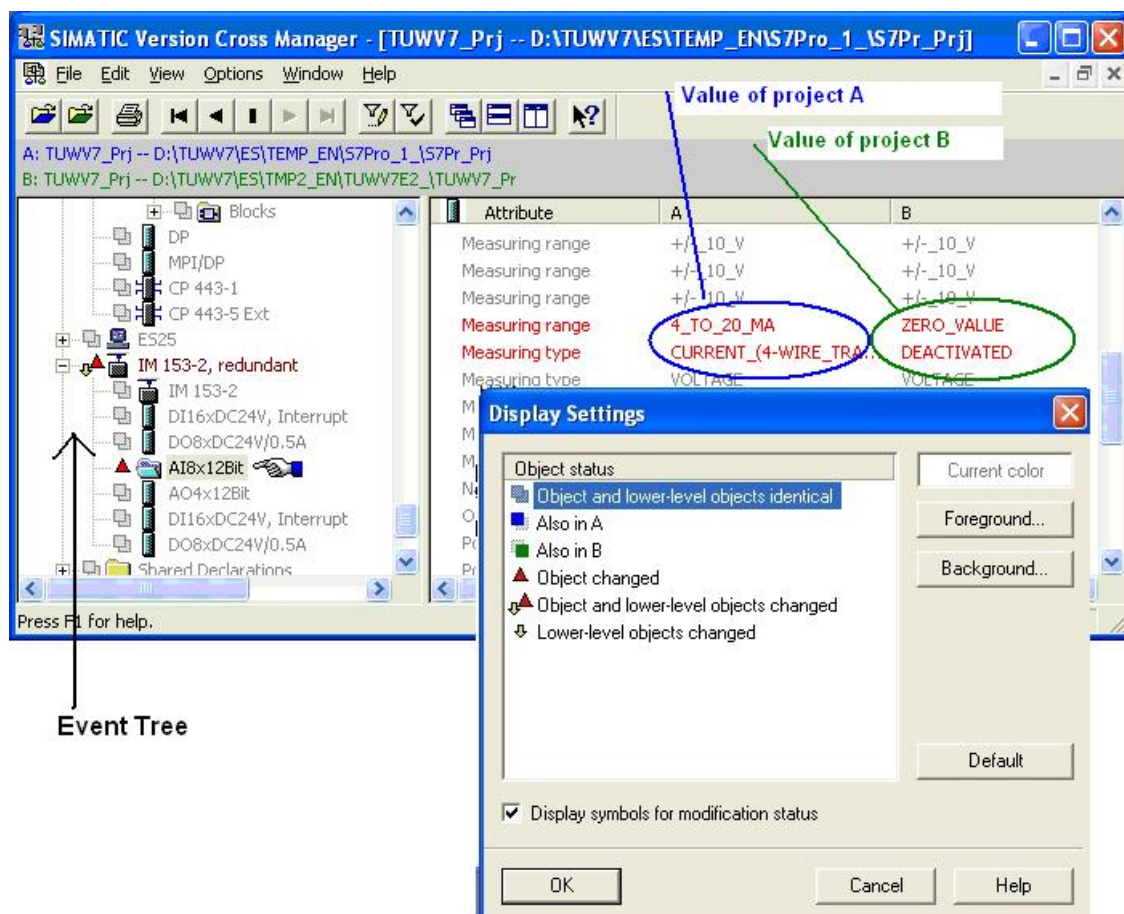
All software versions are listed in chronological order, together with their archiving date and version. This ensures that the latest software version can be copied back should the application software be lost.

## 7.4.2 Change Control with “Version Cross Manager” (VXM)

The Version Cross Manager compares the following objects within projects:

- Hardware configuration
- CFC/SFC engineering data such as block charts, types, chart folders, block folders
- Shared declarations
- Block sequences
- S7 program
- S7 blocks
- S7 symbols

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.



The color display setting can be customized.

### **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 following information is displayed:

- Additional objects contained in project A
- Additional objects contained in project B
- Differences between project A and project B

### **Application Examples for the VXM**

Scenario 1: The Version Cross Manager can be used to verify that a change has been implemented correctly in the context of the change control system, for example. Comparing the software version prior to the change with the current program version in the automation system's CPU shows what changes have been made to the system; these changes must comply with the corresponding change specification.

Scenario 2: Another use of the Version Cross Manager is for verifying that an archived software version matches the current program version in the automation system's CPU. When the current software backup is compared with the automation system, there must be no deviations between the software backup and the automation system's CPU, unless a change request has been submitted.

See also information about "Change Control during Operation" in chapter 8.2.

## 8 Operation, Service and Maintenance

### 8.1 Asset Management

#### Introduction

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 out where and at what time.

#### Implementation in PCS 7

SIMATIC PCS 7 and its integrated Asset Management system are used for plant maintenance. This option is integrated in the PCS 7 process control system and runs there in parallel with plant automation. 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. The PCS 7 operator station (OS) operator control and monitoring functions provide the plant operator with all process-relevant information, allowing him to make targeted interventions in the process. By contrast, the maintenance engineer uses the maintenance station (MS) to monitor the hardware structure of the production plant, allowing him to meet diagnostic and maintenance requirements. Individual events in the hierarchy tree of the hardware structure are also shown – diagnostic data is displayed using faceplate technology, any maintenance requests are made visible by clicking the mouse.

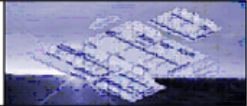
The diagnostic and maintenance functions integrated in SIMATIC PCS 7 allow the different components of a PCS 7 plant to be monitored and the status to be displayed. This status is shown using defined standardized symbols. In addition to the standardized symbols, it is important for the overview to have a hierarchical information structure from which the maintenance engineer can also access all details of the components and devices if necessary, starting from 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. The collective condition message shows the OK condition or the seriousness of a possible problem in red, yellow, or green, as per a traffic light.

The maintenance view of the diagnostic faceplate of a monitored component is where the operator responds to a maintenance request relating to that component. Maintenance work can be requested. The status of the work can also be specified.



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.

A report can be printed out for each component.

SIMATIC Asset Report	
Copyright (c) 1994-2007 by SIEMENS AG	
	
<b>Tag</b>	<b>SIPART PS2A PA</b>
<b>Status</b>	<b>Maintenance required</b>
Description	Positioner
Message	GMP Manual
Device type	SIPART PS2 PA
Manufacturer	Siemens
Order Number	
Serial number	120039
Install date	01.01.2001
HW-Revision	FBG 6 LP 9
SW-Revision	5.00.00-00 / E1
<b>Request number</b>	<b>4711</b>
<b>Request Operator</b>	<b>Demand</b>
Note	strokes exceeded, check valve
PDM Diagnose	>> Maintenance required <<
PDM Diagnose	- Limit for stroke integral (full strokes) exceeded (Limit 1).
PDM Diagnose	The total distance travelled by the actuator exceeded the set limit value.
PDM Diagnose	Actual number of strokes: 1
PDM Diagnose	-> Check valve and actuator, e.g. packing / stuffing box, diaphragma.

Date	Time	Event
12/09/2007	13:15:10	Device 3/7/42: good, maintenance need

ES13	9/12/2007 11:20:54 AM
OHIO	1 / 1

## Condition Monitoring

It is often necessary to take particular process-engineering, chemical, and mechanical conditions into account 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.

## 8.2 Change Control during Operation

It is essential that all changes to be made to validated, operational plants are planned in consultation with the process owner, documented, and only executed and tested once they have been released.

A change procedure used for change control during operation would include the steps below, using the example of a software change:

- Initiate and describe the change, which is released by operator
- Verify the current software using the Version Cross Manager and an online comparison
- Adapt the system specification, in the FS, for example
- Execute and document the change
- Verify the changes using the Version Cross Manager and an online comparison
- Test the change and create appropriate test documentation

## 8.3 Remote Maintenance

As of PCS 7 version V7.0, the Microsoft NetMeeting product is the recommended tool to use for remote access. It forms part of the operating system and does not have to be installed as an additional component.

Essentially, a connection to an external PC station can be established via a modem, ISDN, xDSL, or a network. 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.

---

### Note

In a controlled GMP environment, many control systems are configured as closed systems or “isolated applications”. Thorough discussions must be held with the process owner before remote maintenance functionality is set up. Those responsible for the plant must give their express consent for each individual connection to the system (logon).

---

A practical solution could be to assign the logical access permission, but to only establish a physical connection if necessary, and then only when on-site maintenance staff is present.

---

### Note

As NetMeeting is capable of encrypting data transmissions, the user should make sure that encryption is activated, particularly when sending data via an Internet connection.

---

## 8.4 Date Retrieval

The procedure described in this chapter should enable the system owner to retrieve lost data or to rebuild the system after a system breakdown.

Such a disaster or system breakdown could be caused by:

- Damage of operating system or installed programs
- Damage of system configuration or engineering data
- Loss or damage of runtime data

Based on the backup data, the system is to be rebuilt. The backup media and all other necessary data for system reconstruction (operating system, images, software packages, application software, documentation, etc.) must be located at a defined place. Moreover a disaster recovery plan must exist, be available, and be checked regularly.

### Rebuilding Operating System and Installed Software Packages

Rebuilding the operating system and the installed software packages usually can be done by re-installing the respective Image file, see chapter 6.11 "Data Backup". The installation manuals of the respective tool manufacturers are to be regarded.

If no PC identical in construction is available, the system has to be installed completely new. The existing documentation for qualification of the software can be used, where the installed software and updates and hot fixes are described.

### Rebuilding the Application Software

The reconstruction of the application software depends on the system configuration and the kind type of created software backups.

- *Retrieve data via "Version Trail" software tool*  
Version Trail lists all major and minor version backups including time stamp. For retrieval select the respective version and select de-archiving.
- *Retrieve data from manually created backups*  
Manually created backup copies can also be used for data retrieval.
- *Retrieval of recipes*
- *Retrieval of archives*  
Depending on the system configuration and the degree of system breakdown, process data, event data, batch data, log files, etc. have to be retrieved, too.

### Project Specific Adaptation

Project specific software or configuration adaptations, which are not saved inside the project file, also must be re-installed.

## 9 System Updates and Migrating

### 9.1 Updates, Service Packs and Hotfixes

It is essential that system software updates to be performed on a validated, operational plant are agreed with the process owner. 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 found in chapter 8.2, this roughly translates to the following steps:

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

In considering possible influences, the following may be relevant:

- Modules / typicals / instances / blocks / alarm system in terms of function and display
- Interfaces
- Effects during download
- System performance
- Documentation (specifications)
- Qualification tests to be repeated or performed for the first time

---

#### Note

Support for software updates and project migration is given by SIMATIC Customer Support under <http://support.automation.siemens.com>

---

## 9.2 Migrating to PCS 7

Over the next few years, many plants will have to be thoroughly modernized or, at the very least, expanded in order to deal with their old system components, which are no longer supported. For this reason, the issue of migration, which refers to the transition to a new generation of products featuring updated technology, is becoming more and more important for a number of plants, particularly in terms of process control engineering.

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.

A customized migration strategy is designed, taking the necessary qualification measures into account and based on the relevant general conditions, such as the basis which is already installed and on which the migration is to take place, defined plant stoppages (usually as brief as possible), etc.

# Index

## A

Access Protection 13  
Alarm Management 104  
Application software backup 21  
Approval and change procedure 8  
Archiving 17, 121  
Asset Management 149  
Audit trail 16  
Audit Trail 109

## B

Basic Software 29  
Batch documentation 18  
Batch report 100  
Batch reporting 18  
Biometric systems 14

## C

CAS 123  
Central archive server 34  
Change Control 11, 109, 151  
Configuration Control 11  
Configuration Identification 11  
Configuration Management 10

## D

Data Backup 21, 99, 119  
Date Retrieval 152  
Design Specification 4

## E

Electronic batch data 19  
Electronic record 20  
Electronic Records 121  
Electronic signature 15  
Electronic Signature 116  
EU-GMP Guide 6  
EU-GMP Guide – Annex 11 7  
EU-GMP Guide - Annex 18 7

## F

FAT 4  
FDA 21 CFR Part 11 6

FDA sets of regulations 7  
Foundation Fieldbus 70  
Functional Specification 3

## G

GAMP 6, 7  
GAMP Good Practice Guide 7  
Guidelines 6

## H

Hardware categorization 9  
Hardware Specification 26

## I

Implementation 4  
Import Export Assistant 89  
Information Security 53  
ISA-88.01 96, 97

## L

Life cycle model 1

## M

Maintenance 149  
Manufacturing log 19  
Master Data Library 58  
Migration 154  
Multiproject 55

## N

NAMUR recommendation 7

## O

Open PCS 7 93  
Operating system 29  
OS archiving 28, 32

## P

Password 14, 16  
PCS 7 OS Web 92  
PDM 68  
Printer drivers 36

Process data backup 23  
PROFIBUS 63

## Q

Qualification 5, 135, 136, 142  
Qualification plan 2  
Qualification Report 5  
Quality and project plan 3

## R

Referenced OS Stations 57  
Regulations 6  
Remote Maintenance 151  
Retrieving archived data 23  
Route Control 102

## S

SAT 4  
Scripts 91  
Selecting hardware 26  
SIMATIC BATCH 33, 48, 95, 98, 116  
SIMATIC Logon 48  
Simulation 143  
Smart card 14  
Software categorization 10  
Software Categorization 138

Software creation 12  
Specification 3  
StoragePlus 34, 127

## T

Third-party component 24  
Time synchronization 17  
Typicals 12, 84

## U

Uninterruptible power supply – Configuration 131  
Uninterruptible Power Supply (UPS) 130  
Updates 153  
User Administration 38  
User ID 14, 16  
User Management 13  
User requirements specification 3  
User Rights 44

## V

Validation plan 2  
Validation Report 5  
Version Trail 144  
Versioning 11, 75  
Virus scanners 36

A5E02147608-01

**Siemens AG**

Automation and Drives  
Competence Center Pharmaceuticals  
76181 KARLSRUHE  
GERMANY

[pharma.aud@siemens.com](mailto:pharma.aud@siemens.com)  
[www.siemens.com/simatic-pcs7](http://www.siemens.com/simatic-pcs7)