Safety Guidelines

This manual contains notices intended to ensure personal safety, as well as to protect the products and connected equipment against damage. These notices are highlighted by the symbols shown below and graded according to severity by the following texts:

Danger
indicates that death, severe personal injury or substantial property damage will result if proper precautions are not taken.

Warning
indicates that death, severe personal injury or substantial property damage can result if proper precautions are not taken.

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

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

Notice
draws your attention to particularly important information on the product, handling the product, or to a particular part of the documentation.

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.

Correct Usage

Note the following:

Warning
This device and its components may only be used for the applications described in the catalog or the technical description, and only in connection with devices or components from other manufacturers which have been approved or recommended by Siemens.

This product can only function correctly and safely if it is transported, stored, set up, and installed correctly, and operated and maintained as recommended.

Trademarks

SIMATIC®, SIMATIC HMI® 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.

Copyright © Siemens AG 2004 All rights reserved

The reproduction, transmission or use of this document or its contents is not permitted without express written authority. Offenders will be liable for damages. All rights, including rights created by patent grant or registration of a utility model or design, are reserved.

Disclaimer of Liability

We have checked the contents of this manual for agreement with the hardware and software described. Since deviations cannot be precluded entirely, we cannot guarantee full agreement. However, the data in this manual are reviewed regularly and any necessary corrections included in subsequent editions. Suggestions for improvement are welcomed.

Siemens AG
Bereich Automation and Drives
Geschaeftsgebiet Industrial Automation Systems
Postfach 4848, D- 90327 Nuernberg

Siemens Aktiengesellschaft

©Siemens AG 2004
Technical data subject to change.

ASE00158475-02
Preface

Purpose of the Manual

This manual will inform you about the basic solution concept, the method of operation and the most important configurations to be made when building fault-tolerant systems using the SIMATIC PCS 7 process control system. It presents fault-tolerant solutions on all automation levels (control, process, field).

We may refer to other product manuals for information which specifically deals with the handling of individual components.

Required Knowledge

General knowledge in the area of automation engineering and basic knowledge of PCS 7 is required to understand this manual. It is assumed that the reader knows how to use computers or other equipment similar to PCs (such as programming devices) operating under the Windows 2000 operating system.

The Configuration Manual and the Getting Started section will provide you with the basics regarding the use of PCS 7.

Scope of this Manual

This manual applies to the software package, SIMATIC PCS 7 V6.0.
Organization of the Documentation

The following documentation provides more information about fault-tolerant process control systems and the handling of the individual components. These documents are components of the Manual CD, "Process Control System PCS 7 V6.0, Electronic Manual".

<table>
<thead>
<tr>
<th>Manual</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Getting Started Process Control System PCS 7; Part 1</td>
<td>Part 1: Creating the Project Working with the CFC Editor Working with the Import/Export Assistant Working with the SFC Editor Compiling, Downloading and Testing Working with the Operator Station</td>
</tr>
<tr>
<td>SIMATIC Process Control System PCS 7 Configuration Manual; Engineering System</td>
<td>Basics of PCS 7 Creating the Project Configuring Hardware Configuring Networks</td>
</tr>
<tr>
<td>SIMATIC Process Control System PCS 7 Configuration Manual; Operator Station</td>
<td>Configuring SIMATIC Connections Connecting OS Blocks Configuring Operator Station Compiling OS Installation Guidelines</td>
</tr>
<tr>
<td>WinCC Configuration Manual</td>
<td>Getting Started Operation of Redundancy User Archive Creation of the Project_Redundancy_Server Project Description of the WinCC Projects Server Project</td>
</tr>
<tr>
<td>Manual for Software Update PCS 7 V6.0</td>
<td>Updating a PCS 7 Project With and Without Utilization of New Functions Upgrading a Redundant System During Online Operation</td>
</tr>
<tr>
<td>Manual Automation System S7-400H, Fault-Tolerant Systems</td>
<td>Redundant Programmable Logic Controllers in the SIMATIC Series Increasing System Availability System and Operating Modes of the S7-400H Link-up and Update</td>
</tr>
<tr>
<td>Manual Modification of the System during Operation via CiR</td>
<td>Modification of the Standard Systems during Operation</td>
</tr>
</tbody>
</table>
Directory

This manual is organized according to the following topics:

- Chapter 1 explains the basics of fault tolerance in PCS 7.
- Chapter 2 presents fault-tolerant solutions in PCS 7.
- Chapter 3 describes the configuration of various components in PCS 7 when used in a fault-tolerant architecture.
- Chapters 4 and 5 present failure scenarios and the available diagnostic methods.
- Chapter 6 explains the possibilities for quantitative analysis of fault-tolerant control systems.
- The glossary contains important terms to help you better understand this documentation.
- The index will aid you in quickly locating detailed information associated with important key words.
Preface

Further Support

If you have any technical questions, please get in touch with your Siemens representative or agent responsible.

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

Training Centers

Siemens offers a number of training courses to familiarize you with the Process Control System SIMATIC PCS 7 and the SIMATIC S7 automation system. Please contact your regional training center or our central training center in D 90327 Nuremberg, Germany for details:
Telephone: +49 (911) 895-3200.
Internet: http://www.sitrain.com
A&D Technical Support
Worldwide, available 24 hours a day:

<table>
<thead>
<tr>
<th>Worldwide (Nuernberg) Technical Support</th>
<th>United States (Johnson City) Technical Support and Authorization</th>
<th>Asia / Australia (Beijing) Technical Support and Authorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>24 hours a day, 365 days a year</td>
<td>Local time: Mon.-Fri. 8:00 to 5:00 PM</td>
<td>Local time: Mon.-Fri. 8:00 to 5:00 PM</td>
</tr>
<tr>
<td>Phone: +49 (180) 5050-222</td>
<td>Phone: +1 (423) 262 2522</td>
<td>Phone: +86 10 64 75 75 75</td>
</tr>
<tr>
<td>Fax: +49 (180) 5050-223</td>
<td>Fax: +1 (423) 262 2289</td>
<td>Fax: +86 10 64 74 74 74</td>
</tr>
<tr>
<td>E-Mail: <a href="mailto:adsupport@siemens.com">adsupport@siemens.com</a></td>
<td>E-Mail: <a href="mailto:simatic.hotline@sea.siemens.com">simatic.hotline@sea.siemens.com</a></td>
<td>E-Mail: <a href="mailto:adsupport.asia@siemens.com">adsupport.asia@siemens.com</a></td>
</tr>
<tr>
<td>GMT: +1:00</td>
<td>GMT: -5:00</td>
<td>GMT: +8:00</td>
</tr>
</tbody>
</table>

The languages of the SIMATIC Hotlines and the authorization hotline are generally German and English.
Service & Support on the Internet

In addition to our documentation, we offer our Know-how online on the internet at: http://www.siemens.com/automation/service&support

where you will find the following:

• The newsletter, which constantly provides you with up-to-date information on your products.

• The right documents via our Search function in Service & Support.

• A forum, where users and experts from all over the world exchange their experiences.

• Your local representative for Automation & Drives. Information on field service, repairs, spare parts and more under "Services".
Contents

1 Basics of Fault Tolerance 1-1
   1.1 Reasons for Using Fault-tolerant Process Control Systems .................... 1-1
   1.2 Analyzing Fault Tolerance throughout the Plant .................................. 1-4
   1.3 SIMATIC PCS 7 Redundancy Concept ..................................................... 1-5
   1.4 Overview of SIMATIC PCS 7 Features .................................................. 1-9
   1.5 Features for the Configuration Phase .................................................... 1-10
   1.6 Features for Commissioning and Operation Phase ............................... 1-11
   1.7 Features for Servicing and System Expansion ........................................ 1-13
   1.8 Definition of Fault Tolerance ............................................................... 1-13
   1.9 Redundancy Nodes .............................................................................. 1-14

2 Fault-tolerant Solutions in PCS 7 2-1
   2.1 Solutions for I/O .................................................................................. 2-1
      2.1.1 Solutions for I/O ........................................................................... 2-1
      2.1.2 Single-channel Switched Distributed I/O .......................................... 2-3
      2.1.3 Redundant I/O .............................................................................. 2-4
      2.1.4 Design and Configuration Rules ...................................................... 2-6
      2.1.5 Distributed I/O Device ET 200M ..................................................... 2-6
      2.1.6 Expansion components for ET 200M .............................................. 2-7
      2.1.7 Redundant Interface Module IM 153-2 .......................................... 2-7
      2.1.8 Redundant I/O Modules .................................................................. 2-7
      2.1.9 DP/PA-Link ................................................................................. 2-9
      2.1.10 Y-Link ..................................................................................... 2-11
      2.1.11 PROFIBUS Connection to the Automation Station ....................... 2-12
      2.1.12 Redundant Actuators and Sensors ............................................... 2-12
   2.2 Solutions for Automation Systems ....................................................... 2-13
      2.2.1 Solutions for Automation Systems ................................................ 2-13
      2.2.2 S7-400H Hardware Components .................................................. 2-14
      2.2.3 How the S7-400H Operates ............................................................ 2-16
   2.3 Solutions for Communication ............................................................... 2-17
      2.3.1 Solutions for Communication ........................................................ 2-17
      2.3.2 Redundant Field Bus ..................................................................... 2-20
      2.3.3 Redundant System Bus .................................................................. 2-22
      2.3.4 Redundant Terminal Bus ............................................................... 2-26
   2.4 Solutions for OS Servers ...................................................................... 2-29
      2.4.1 Redundant OS Servers ................................................................. 2-29
      2.4.2 Time Synchronization .................................................................. 2-31
      2.5 Solutions for SIMATIC BATCH .......................................................... 2-34
      2.5.1 Redundant BATCH Servers ............................................................ 2-34
      2.6 Solutions for OS Clients .................................................................... 2-38
      2.6.2 Additional OS Clients .................................................................... 2-38
      2.6.3 Engineering Station (ES) ............................................................... 2-39
3 Configuring Fault-tolerant Components

3.1 Notes about Configuring Fault-tolerant Components ........................................... 3-1
3.2 SIMATIC H Station .................................................................................................. 3-2
3.2.1 How to Insert a SIMATIC H Station into Your Project ........................................ 3-2
3.2.2 How to Insert Synchronization Modules into the Fault-tolerant CPU ................. 3-3
3.2.3 How to Configure Redundant Communication Processors .............................. 3-5
3.3 Configuring Communication Connections ............................................................ 3-7
3.3.1 How to Configure a Redundant Field Bus .......................................................... 3-10
3.3.2 How to Configure a Redundant System Bus ...................................................... 3-13
3.3.3 How to Configure a Redundant Terminal Bus ................................................... 3-15
3.4 Distributed I/O ...................................................................................................... 3-16
3.4.1 How to Configure the Redundant IM 153-2 Interface Module for an ET 200M I/O Device .................................................................................................................. 3-16
3.4.2 How to Configure Redundant I/O Modules ......................................................... 3-18
3.4.3 How to Configure the Y-Link ............................................................................ 3-21
3.4.4 How to Configure the DP/PA-Link ................................................................... 3-24
3.4.5 How to Import GSD Files ................................................................................ 3-27
3.5 SIMATIC PC Stations ............................................................................................ 3-28
3.5.1 How to Configure an OS Server and Its Redundant OS Partner Server ............... 3-28
3.5.2 How to Set the Project Paths of the Destination OS and Standby OS ............... 3-30
3.5.3 How to Configure a Redundant Connection Between an OS and AS .............. 3-31
3.5.4 How to Assign an S7 Program to an OS ............................................................ 3-33
3.5.5 How to Configure WinCC Redundancy ............................................................... 3-34
3.5.6 How to Download a SIMATIC PCS 7 Project to PLCs ..................................... 3-36
3.5.7 How to Configure an OS Client ....................................................................... 3-37
3.5.8 How to Configure an OS Client for Continuous Operations ............................ 3-39
3.5.9 How to Synchronize the Time on OS Clients to OS Servers ............................ 3-41
3.5.10 How to Synchronize the Time on OS Servers to an External Time Generator ...... 3-43
3.6 SIMATIC BATCH ................................................................................................. 3-45
3.6.1 How to Configure a PC Station for a Redundant BATCH Server ....................... 3-45
3.6.2 How to Configure a PC Station for a BATCH Client .......................................... 3-47
3.7 Component Replacement and System Modifications ............................................. 3-49
3.7.1 Replacing Components During Online Operation ........................................... 3-49
3.7.2 Modification of the Standard Systems During Online Operation .................... 3-50

4 Failure, Failover and Restarting Fault-tolerant Components

4.1 I/O Modules .......................................................................................................... 4-1
4.1.1 Redundant Interfaces .................................................................................... 4-1
4.1.2 Redundant I/O Modules ................................................................................ 4-2
4.2 Automation Systems ........................................................................................... 4-5
4.2.1 Failure of the Master CPU ............................................................................ 4-3
4.2.2 Failure of a Fiber-Optic Cable ....................................................................... 4-4
4.3 OS Servers .......................................................................................................... 4-6
4.3.1 Failure, Failover and Restarting of Redundant OS Servers .............................. 4-6
4.4 BATCH Servers .................................................................................................. 4-11
4.4.1 Failure reactions of BATCH servers ............................................................... 4-11
4.5 OS Clients .......................................................................................................... 4-12
4.5.1 Failover Reactions of OS Clients for Continuous Operations ........................... 4-12
4.6 BATCH Clients ................................................................................................... 4-14
4.6.1 Failover Reactions of BATCH Clients ............................................................ 4-14
### Contents

#### 5 Diagnostics
- 5.1 Diagnostics for Redundant Components and Systems ........................................ 5-1
- 5.2 Reporting, Testing and Monitoring .................................................................... 5-2
- 5.2.1 Hardware Diagnostics .................................................................................... 5-2
- 5.2.2 WinCC Diagnostics ....................................................................................... 5-3
- 5.2.3 Lifebeat Monitoring ..................................................................................... 5-5
- 5.2.4 WinCC Scope ................................................................................................ 5-7
- 5.2.5 NetCC ............................................................................................................ 5-9

#### 6 Parameters of Fault-tolerant Process Control Systems
- 6.1 Parameters of Fault-tolerant Process Control Systems ...................................... 6-1

<table>
<thead>
<tr>
<th>Glossary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
</tr>
</tbody>
</table>
1 Basics of Fault Tolerance

1.1 Reasons for Using Fault-tolerant Process Control Systems

Process control systems are responsible for controlling, monitoring and documenting production and finishing processes. Due to the increasing degree of automation and the demand for improved efficiency, the fault tolerance of these systems is playing an increasingly important role.

Failure of the control system or any of its components can lead to costly downtime in production and finishing. The expense involved in restarting a continuous process also has to be taken into consideration along with the actual production losses resulting from a failure. In addition, the loss of an entire batch may occur due to lost quality data. If the process is intended to operate without supervisory or service personnel, all of the components in the process control system needs to be fault-tolerant.

The use of fault-tolerant components in a process control system can minimize the risk of a production shutdown. A redundant design guarantees fault tolerance in a control system. This means that all components involved in the process have a backup in continuous operation that simultaneously participates in the control tasks. When a fault occurs or one of the control system components fails, the correctly operating redundant component takes over the continuing control task. The ultimate goal is to increase the fault tolerance and error protection in process control systems.

As the plant operator you should consider that the higher the cost of a production failure, the more you need a fault-tolerant system. The higher initial investment usually associated with a fault-tolerant system is quickly offset by the savings resulting from decreased production downtime.
PCS 7 Process Control System

The components of the PCS 7 process control system enable you to assign any degree of fault tolerance to all automation levels, from operator stations (management level) to the bus system, from the automation system (process level) to the distributed I/O (field-I/O level). The following illustration shows a fault-tolerant process control system with PCS 7 components.
Legend for the above illustration:

**Note**
The following short designations are commonly used in this documentation.

<table>
<thead>
<tr>
<th>Short Designation</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>ES</td>
<td>Engineering station, PC</td>
</tr>
<tr>
<td>OS server</td>
<td>Operator station, PC project data station in the project form &quot;WinCC Server&quot;</td>
</tr>
<tr>
<td>OS client</td>
<td>Operator station, PC visualization station in the project form &quot;WinCC Client&quot;</td>
</tr>
<tr>
<td>BATCH Server</td>
<td>PC recipe and batch data station</td>
</tr>
<tr>
<td>BATCH Client</td>
<td>PC recipe creation and batch visualization station</td>
</tr>
<tr>
<td>PC network</td>
<td>Ethernet communication in electronic or optical form</td>
</tr>
<tr>
<td>Industrial Ethernet</td>
<td>Communication via industrial Ethernet in electronic or optical form</td>
</tr>
<tr>
<td>S7-400H</td>
<td>SIMATIC S7 fault-tolerant automation system</td>
</tr>
<tr>
<td>PS</td>
<td>Power supply</td>
</tr>
<tr>
<td>CPU</td>
<td>Central processing unit</td>
</tr>
<tr>
<td>CP</td>
<td>Communication processor</td>
</tr>
<tr>
<td>IM</td>
<td>Interface module</td>
</tr>
<tr>
<td>SM</td>
<td>Analog or digital signal (I/O) module</td>
</tr>
<tr>
<td>ET 200M</td>
<td>Distributed I/O device</td>
</tr>
<tr>
<td>Y-Link</td>
<td>Interface to allow non-redundant PROFIBUS-DP devices to be connected to redundant DP segments</td>
</tr>
<tr>
<td>DP/PA Link</td>
<td>Transceiver</td>
</tr>
<tr>
<td>PROFIBUS-DP</td>
<td>PROFIBUS distributed I/O</td>
</tr>
<tr>
<td>PROFIBUS-PA</td>
<td>PROFIBUS process automation</td>
</tr>
<tr>
<td>Sensor</td>
<td>Signal encoder, sensor</td>
</tr>
</tbody>
</table>
1.2 Analyzing Fault Tolerance throughout the Plant

Tolerance should be analyzed globally throughout the plant. Once a decision is made about the degree of tolerance needed, each system level, each system and each component within a level should be evaluated for its role in the fulfillment of these requirements. Then decisions need to be made about the ways and means to achieve this degree of availability.

Repair Time

In many industrial processes it is not enough to simply correct the failure of a component and then restart the process. The repair has to be made without interruption to the production process while it is online. The repair time can be considerably reduced by keeping replacement parts in stock on site. Even better, the repair time can be completely eliminated by the use of fault-tolerant components in the process control system. The failure of the system or a component can then be remedied during online operation.

Bumpless Transfer of Components after Repair

Another consideration involves bumpless transfer of components after repairs, in other words, the avoidance of spurious transitions at the outputs during the failover to a backup system with connected backup I/Os.
1.3 SIMATIC PCS 7 Redundancy Concept

Fault-tolerant process control systems for SIMATIC PCS 7 can be realized at minimal cost for all phases of a plant lifecycle - configuration, commissioning/operation, servicing and upgrading. SIMATIC PCS 7 offers you a redundancy concept that reaches all levels of process automation.

SIMATIC PCS 7 offers the following basic benefits:

- It provides you with system-wide scalable solutions from the SIMATIC PCS 7 modular system, which you can use to meet the exact demands placed on your process control system.  
  Benefit: Matches the availability to your requirements. Your process control system is upgraded by only the SIMATIC PCS 7 components that are actually needed.

- Hardware upgrades for fault tolerance do not depend on the software configuration.  
  Benefit: If the user program has been configured with SIMATIC PCS 7, it does not have to be adapted following a hardware upgrade. You only need to load the new hardware configuration into the CPU.

- The fault-tolerant S7-400 H automation system with the CPU’s 414-4H and 417-4H, whose mounting racks can be spatially separated.  
  Benefit: Protection for the spatially separated CPU’s against fire or explosion.

- The use of redundant components in the process control system means isolated errors are tolerated.  
  Benefit: The entire system does not fail when a single component in the process control system fails. The redundant component takes over its tasks therefore allowing the process to continue.

- Every failure of a redundant component is reported at the OS client in the form of a control message.  
  Benefit: You receive without delay critical information about the status of your redundant component. Faulty components can be quickly exchanged to restore the redundancy.

- Software updates on redundant OS servers can be carried out without losing control of the process and loss of data.
SIMATIC PCS 7 Redundancy Concept

1. OS Client
2. Optical Switch Module (OSM) with integrated redundancy features
3. Double redundant system bus (Fast Ethernet)
4. Synchronization line
5. Fault-tolerant automation system with CPUs:
   a. AS 414 H
   b. AS 417 H
6. Spatially separated mounting racks
7. Sensor
8. PROFIBUS-DP Y coupler
9. Y link with two IM 157
Note
The numbering of the components in the illustration relates to the descriptions listed below.

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The data on the OS server can be accessed by more than one OS client.</td>
</tr>
<tr>
<td>2</td>
<td>The OS server itself can be installed with redundancy if required.</td>
</tr>
<tr>
<td>3</td>
<td>The communication between the automation systems and the OS server and engineering stations, as well as the communication amongst themselves, is made via the redundant industrial Ethernet bus which can be operated at 10 or 100 Mbaud.</td>
</tr>
<tr>
<td>4</td>
<td>The redundant automation system S7-400H with the CPU's AS 414 H or AS 417 H is connected with an Ethernet communication processor (CP) to each automation subsystem. Each standard AS, OS and ES systems are connected to the system bus with only one CP. Using the internal PROFIBUS-DP interface or other communication processors, several PROFIBUS-DP master systems can be connected to distributed I/O from each automation subsystem. Centralized I/O can also be used in the mounting rack of the S7-400H.</td>
</tr>
<tr>
<td>5</td>
<td>A redundant connection to the PROFIBUS-DP master system can be made using the two 153-2 IM's in each ET 200M.</td>
</tr>
<tr>
<td>6</td>
<td>The PROFIBUS-PA I/O is connected to the redundant PROFIBUS-DP by DP/PA-Link and two 157 IM's.</td>
</tr>
<tr>
<td>7</td>
<td>Using redundant digital or analog input modules you can evaluate sensor signals and, when one of the two input modules fails, the sensor signal of the other input module is used. Digital and analog output modules are connected according to the same principle.</td>
</tr>
<tr>
<td>8</td>
<td>The Y-link enables you to connect non-redundant distributed I/O devices to a redundant field bus.</td>
</tr>
</tbody>
</table>
Illustration of Fault Tolerance Using Redundancy Nodes

Redundancy nodes can be used to provide an overview of the process control system’s fault tolerance. The following illustration presents the process control system shown above as a block diagram with the individual redundancy nodes as an example.

Note
The terminal bus, marked with * in the block diagram shown above, can be installed redundantly with optical or electronic switch modules. This means that a broken cable in the redundant OS-LAN will be tolerated and will not result in restricted communication between the OS client and OS server. When a single switch module is installed and it fails, however, the communication with the connected nodes will be disrupted.

Further Topics
Definition of Fault Tolerance
Redundancy Nodes
1.4 Overview of SIMATIC PCS 7 Features

The easiest way to increase availability is to keep replacement parts in stock on site and to have fast service at your disposal to replace defective components. SIMATIC PCS 7 provides software and hardware solutions that go well beyond fast service and local stock. It focuses on "automated fault-tolerant process control systems".

Our goal here is to meet your demands and those of your customers for fault-tolerant process control systems, i.e., services and scalable solutions specifically designed to increase the availability in your plant.

The SIMATIC PCS 7 process control system fulfills these demands for fault-tolerant process control systems. The components of SIMATIC PCS 7 enable you to realize fault-tolerant solutions on all automation system levels in the form and to the degree you desire.

PCS 7's Comprehensive Solution

The SIMATIC PCS 7 process control system is a comprehensive system and its components are finely matched to one another. The HMI extends throughout the system from sensors to actuators and guarantees the highest system performance.

Stepped, Scalable Fault Tolerance through Redundant Components

PCS 7 increases fault tolerance by using redundancy for all critical components and by supporting the corresponding software mechanism. The components in SIMATIC PCS 7 can be divided into the field-I/O level, process level and management level (HMI). SIMATIC PCS 7 offers a solution for every component on these levels. The following table lists the three levels and the corresponding fault-tolerant hardware components.

<table>
<thead>
<tr>
<th>Process level</th>
<th>Components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management (HMI)</td>
<td>• OS clients; BATCH clients</td>
</tr>
<tr>
<td></td>
<td>• OS server, BATCH server</td>
</tr>
<tr>
<td></td>
<td>• Terminal bus (Industrial Ethernet, Fast Ethernet)</td>
</tr>
<tr>
<td>Process</td>
<td>• System bus (Industrial Ethernet, Fast Ethernet)</td>
</tr>
<tr>
<td></td>
<td>• Automation system AS 414H, AS 417H</td>
</tr>
<tr>
<td></td>
<td>• Central I/O modules of the S7-400 series</td>
</tr>
<tr>
<td>Field-I/O</td>
<td>• Field bus PROFIBUS-DP, PROFIBUS-PA</td>
</tr>
<tr>
<td></td>
<td>• Distributed I/O device ET200M</td>
</tr>
<tr>
<td></td>
<td>• Distributed I/O modules of the S7-300 series</td>
</tr>
<tr>
<td></td>
<td>• PROFIBUS-DP, PROFIBUS-PA and HART devices</td>
</tr>
</tbody>
</table>

You yourself can decide where to employ redundant components depending on your requirements for fault-tolerance. SIMATIC PCS 7 offers you a solution for scalable, comprehensive and complete fault-tolerance.
1.5 Features for the Configuration Phase

The following table provides you with an overview of the individual features of SIMATIC PCS  7 fault tolerant components for all phases of the plant lifecycle.

Features for the Configuration Phase

In the configuration phase, SIMATIC PCS  7 provides you with support with the following features.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fault prevention through simplified</td>
<td>You do not need additional training to configure the redundant components. The configuration can be carried out in the same way as for a standard system.</td>
</tr>
<tr>
<td>configuration of the various components</td>
<td></td>
</tr>
<tr>
<td>Simplified connection of redundant I/O</td>
<td>No special knowledge is needed about redundant I/O modules.</td>
</tr>
<tr>
<td>devices</td>
<td></td>
</tr>
<tr>
<td>The communication connection between the</td>
<td>Using GUIs such as HW Config or NetPro, the configuration of the communication connections is carried out transparent to the application.</td>
</tr>
<tr>
<td>plant components can be configured</td>
<td></td>
</tr>
<tr>
<td>transparent to the application.</td>
<td></td>
</tr>
</tbody>
</table>
1.6 Features for Commissioning and Operation Phase

The following table lists the features SIMATIC PCS 7 offers for the commissioning and operation phases. The available redundant component takes over the assurance, protection and continuation of the process in case of failure. This enables you to continue to control and monitor your process even when individual components fail. In addition, the archiving of process data is not interrupted during the commissioning phase. Defective components can be replaced during online operation.

Note
When a component fails in a redundant control system, the fault tolerance is lost and a further failure means the failure of the entire system.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefit</th>
<th>Potential Source of Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>Toleration of an isolated error</td>
<td>An isolated error is tolerated since the fault-tolerant redundant component can continue the process.</td>
<td>Fault or failure of OS server or OS client due to such events as hard disk failure, operating system failure, connection failure, hard disk becomes full during archiving. Fault or failure of automation system due to such events as power failure, CPU stop at an asynchronous error interrupt and missing data handling block (OB 80 to OB 87). Fault or failure of communication, for example, due to a broken line, electromagnetic compatibility. Fault or failure of central or distributed I/O modules, for example, due to component failure, short circuit. Fault in distributed I/O devices, for example, due to power supply failure (PS), interface module (IM).</td>
</tr>
<tr>
<td>Guarantee of uninterrupted operation through redundant components.</td>
<td>The system can continue control without operator intervention.</td>
<td>Failure of an individual component in a fault-tolerant process control system. Upgrade and expansion of a plant.</td>
</tr>
<tr>
<td>The process can continue to be controlled and monitored even when servers are being changed.</td>
<td>If an OS server fails, the system switches to the configured redundant server. All OS clients are automatically switched to the newly activated OS redundant server. The process can continue to be controlled and monitored through the OS clients even during the failover period.</td>
<td>Failure of the OS server, for example, due to operating system failure or a hard disk defect.</td>
</tr>
</tbody>
</table>
### Basics of Fault Tolerance

#### Feature

<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefit</th>
<th>Potential Source of Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays master / standby identification of the OS server.</td>
<td>The information about the master / standby identification of the OS server can be interrogate and displayed through the OS clients.</td>
<td>The master / standby identification changes when there is a failure of the active OS server (master).</td>
</tr>
<tr>
<td>No data is lost, i.e., a complete data record is guaranteed (archiving).</td>
<td>The project data are saved according to the interval configured.</td>
<td>Failure of the OS server, for example, due to a hard disk defect.</td>
</tr>
<tr>
<td>Continuous operation of the control process through the configuration of a preferred server for each OS client.</td>
<td>The failure of some OS clients can be handled if the remaining clients continue to be connected to the process.</td>
<td>One or more client operator stations fail, for example, due to a hardware or software error. Duration of the failover to OS clients on a redundant OS server</td>
</tr>
<tr>
<td>Replacement of faulty components and reconnection to the system during online operation.</td>
<td>The failed components can be replaced without influencing the ongoing process and subsequently reconnected to the online operation. A redundancy update is then performed.</td>
<td>Failure of an OS client: e.g. operating system Failure of an OS server: e.g. network card Failure of a system bus: e.g. broken cable Failure of central device: e.g. PS, CPU, synchronization line, CP, SM Failure of PROFIBUS-DP: e.g. defective PROFIBUS connector Failure of distributed I/O devices: e.g. PS, IM, SM</td>
</tr>
<tr>
<td>Once a failed component is returned to operation, it is updated with the current system status.</td>
<td>Redundancy synchronization is performed for all fault-tolerant components, for example, a CPU or a server after return to operation.</td>
<td>Failure of a component and subsequent repair. Return of the replaced component, a CPU for example, to the fault-tolerant process control system and subsequent synchronization to the data in the CPU operating in the process</td>
</tr>
<tr>
<td>Upgrading and expanding the plant during online operation</td>
<td>Hardware and software can be upgraded, expanded or exchanged during online operation when redundant components are used in an automation system.</td>
<td>Software update of the OS server Loading the latest firmware into a sectional CPU in STOP mode.</td>
</tr>
<tr>
<td>Safety documentation is possible</td>
<td>Documentation of the availability, for example, debugging and printouts based on MTBF residual time</td>
<td>Identifies and documents potential component failure in advance.</td>
</tr>
</tbody>
</table>
1.7 Features for Servicing and System Expansion

SIMATIC PCS 7 offers the following features for servicing and system expansion:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrated diagnostics of components (e.g. LEDs) for fast, local error detection.</td>
<td>Diagnostics of components without additional programming devices (PG).</td>
</tr>
<tr>
<td>Simple repairs even by untrained operating personnel.</td>
<td>You do not need a specialist on site to carry out repairs.</td>
</tr>
<tr>
<td>Faster service from SIEMENS Customer Support.</td>
<td>The service will be on site within 2-48 hours to maintain the availability guarantee.</td>
</tr>
<tr>
<td>Repair and component installation (upgrades, conversions and updates) during online operation.</td>
<td>Repair and component installation can be made in a fault-tolerant system. System components are installed redundantly so that repairs and installations can be made during online operation.</td>
</tr>
</tbody>
</table>

1.8 Definition of Fault Tolerance

Definitions:
- MTBF - mean time between failure
- MTTR - mean time to repair

Availability is traditionally defined as the quotient MTBF / (MTBF + MTTR) - or in short form: actual operating condition / nominal operating condition.

Increasing the Basic Availability:

Based on this definition, the basic availability of a standard component or a standard system can be increased by:
- Additional improvement to the mean time between failure (MTBF)
- Decreasing the period necessary for repairs (MTTR)

Decreasing the repair time may include the factors servicing proximity to customers, replacement part warehousing, repairs during online operation or repairs without downtime. The "repairs during online operation" factor means, in effect, no repair time is needed in the system to correct unscheduled operation disruptions.
1.9 Redundancy Nodes

Redundancy nodes represent protection from failure in a subsystem through the use of primary and backup components. A redundancy node is considered independent when the failure of one component within the subsystem does not affect the reliability in other nodes or in the entire system.

The fault tolerance of a complete system is illustrated in the block diagram below. In a redundant system, a component in the redundancy node can fail without affecting the operation of the complete system. In the chain of redundancy nodes, the weakest link determines the availability of the entire system. The block diagram below serves as an example to demonstrate this fact.

Redundancy Nodes without Failure

The block diagram shows individual redundancy nodes operating without failure.

Availability of Redundancy Despite Failures

The complete system continues to operate despite the failure of a component in a redundancy node.
Failure of a Redundancy Node (Total Failure)

The diagram shows a complete system which has ceased to operate due to a failure of the "field bus (PROFIBUS-DP)" redundancy node.

Note
The terminal bus mark with * can be installed redundantly with OSM's or ESM's.
2 Fault-tolerant Solutions in PCS 7

2.1 Solutions for I/O

2.1.1 Solutions for I/O

This chapter presents the I/O systems and components that are used to increase the fault-tolerance of your plant. We differentiate between centralized and distributed I/O.

Centralized I/O

When modules (I/O and function modules) are directly installed in the mounting rack of the automation station, we speak of centralized I/O. For the automation system S7-400H you can use almost any input/output module in the SIMATIC PCS 7 product series. If additional module slots are needed, the centralized I/O can be expanded by connecting additional mounting racks (expansion units). A special interface module such as IM 461 can be used to meet your requirements (dismounting, use of CP’s in the expansion units).

The I/O modules (SM) and function modules (FM) available for use in the mounting rack of the S7-400H are listed in Appendix E of the manual Automation System S7-400H; Fault-tolerant Systems.

Distributed I/O

Distributed I/O refers to modules (I/O and function modules), which are used in a modular distributed I/O device such as SIMATIC ET 200M.

Distributed I/O devices are often spatially separate from the automation station and located in direct proximity to the field devices themselves. This minimizes the efforts needed for wiring and the work to ensure the electromagnetic compatibility. The high-performance PROFINET-I/P is used as the communication link between the distributed I/O device and the automation station. An interface module (IM 153-2) in the distributed I/O device serves as the PROFINET-I/P interface.

In addition to I/O devices, distributed I/O also includes field devices such as actuators, weighing systems, motor protection control devices and all other PROFIBUS-capable field devices.

HART devices can be directly connected and addressed through appropriate modules in an ET 200M. HART devices are actuators and sensors that can be configured per HART (Highway Addressable Remote Transducer) protocol.
Bus converters such as DP/PA-Link and user programs are also included in the distributed I/O. DP/PA-Link enables the connection of a lower-level bus system such as PROFIBUS-PA to a redundant PROFIBUS-DP.

An ASi bus can be connected through the ASi communication processors that are used in the distributed I/O device. This enables the connection of simple sensors and actuators of the AS interface to SIMATIC PCS 7. SIMATIC PCS 7 can therefore integrate other I/O levels in a project.

We differentiate between single-channel and redundant I/O. In contrast to redundant I/O, single-channel distributed I/O only has one I/O module (SM) for a process signal.

This chapter focuses on solutions for distributed I/O when used with redundant CPU's.

Increasing System Availability

The availability of I/O modules can be increased by using redundancy within a distributed I/O device and/or by installing an I/O module in two distributed I/O devices. In both cases this is what is meant by redundant I/O. This ensures that the CPU or process signal will continue to be handled by a functioning module even when its partner fails.

Further Topics

- Single-channel switched I/O
- Redundant I/O
2.1.2 Single-channel Switched Distributed I/O

We speak of a single-channel switched configuration when an I/O module can be addressed by both central processing units (CPU's) of a fault-tolerant system. In a single-channel switched configuration there is only one I/O module (single-channel) but it can be addressed through a redundant PROFIBUS-DP.

To configure a single-channel switched I/O you need the distributed I/O device ET 200M with active backplane bus modules and redundant PROFIBUS-DP backup interface module IM 153-2. Each redundancy section of the S7-400H is connected through a DP master interface to one of the two DP backup interfaces of the IM 153-2.

The following illustration shows such a configuration.

The block diagram shows the fault-tolerance of the configuration illustrated above. When both systems are operating without fault, the block diagram appears as follows:

![Block Diagram]

The block diagram shows the fault-tolerance of the configuration illustrated above. When both systems are operating without fault, the block diagram appears as follows:
The following illustration shows how one component may fail without this affecting the operation of the complete system.

The system remains available even when one component in a segment of the redundancy node fails. There is only one I/O module and therefore no corresponding redundancy node. It is the weakest link in the complete system's chain.

2.1.3 Redundant I/O

We speak of redundant I/O when there is more than one I/O module for a process signal and they can be addressed by both central processing units.
The block diagram without fault can be shown with a logical view or component view.

Given a failure in the bus cable (BUS=PROFIBUS-DP) in the first redundancy node and failure of an input module (SM) in the second redundancy node, the complete system continues to operate and the connected sensor continues to supply data to the automation system which remains available. If any other component in the redundancy chain fails, however, this will result in the complete failure of the entire system.
2.1.4 Design and Configuration Rules

Design Rules
The configuration always has to be symmetrical when using single-channel switched I/O. Follow these design rules:

- CPU 41x–4 H and additional DP masters must be located in the same slots of both redundancy sections (for example, in slot 4 of both redundancy sections)
- DP masters in both redundancy sections must be connected to the same integrated interface (for example, to the onboard PROFIBUS-DP interfaces of the two CPU 41x–4 H)

Configuration Rules
- The DP backups (IM 153-2 / IM 157) have to have the same DP address in each ET 200 line.

2.1.5 Distributed I/O Device ET 200M
The distributed I/O device ET 200M is connected as a DP backup through a PROFIBUS-DP to a fault-tolerant automation system operating as the DP master. A redundant configuration is achieved by installing an additional device and an additional PROFIBUS-DP connection. The ET 200M serves as the host for a variety of modules and features its own power supply, which may also be redundant.

The modular distributed I/O device SIMATIC ET 200M for monorail configuration can be equipped and expanded with the following S7-300 modules:

- Power supply (PS)
- Interface module (IM 153-2 and IM 157)
- Signal modules (SM)
- Function modules (FM)

The modules are mounted to a standard rail and interconnected by an integrated backplane bus and bus connector.

Note
When an S7-400H or S7-400 is used as DP master, modules can be removed and inserted during online operation when an active bus module is used in the ET 200M.
2.1.6 Expansion components for ET 200M

The following components are available to expand the distributed I/O device ET 200M for redundancy. Bus modules are required for the active backplane bus to realize a redundant configuration of an ET 200M with two IM 153-2 or IM 153-2 FO interface modules. Eight slots are available for modules in each ET 200M. These are slots 4 to 11 in HW Config.

Expansion Components

- SM modules with single width, whereby two SM modules can be connected to each bus module.
- FM or fail-safe modules with double width, whereby one module can be connected to each bus module.

2.1.7 Redundant Interface Module IM 153-2

A switched distributed I/O configuration can be achieved by employing two IM 153-2 interface modules in a distributed I/O device. Two interface modules are mounted to the bus module in the distributed I/O device for redundant operation. When the active interface module fails, there is a bumpless failover to its backup which takes over the intended functions. The active interface is indicated by an illuminated "ACT" LED on the respective interface module.

2.1.8 Redundant I/O Modules

Redundant I/O modules enable you to considerably increase the fault tolerance of your system. When redundant digital/analog I/O modules are used, an application is not disturbed when a signal fails because it can continue to operate with the redundant signal value. Please note that only specific modules have been released for use as redundant I/O.

Installation and Use

The installation of functional I/O redundancy also activates HW Config for configuration and the library with the function blocks in STEP 7. The blocks can be used in a fault-tolerant process control system. A license is needed for each instance in which the block is used.

Beginning with PCS 7 V6.0, redundant operation of standard modules is possible using the H CPUs (414-H, 417-H) in redundant mode and in single mode with the CPU firmware version V3.1 or later. Redundant operation is possible only with certain modules from the S7-400 and ET200M series.
You will find a list of appropriate modules from both the S7-400 series and the ET200 M series in the manual, Automation System S7 400H; Fault Tolerant Systems. Only modules with the same order number can be paired together in redundant configurations. HW Config is used to select and configure the redundant modules.

In order to address redundant signal modules in both subsystems of the fault-tolerant system, S7 driver blocks from the "Redundant I/O (V1)" library and PCS 7 driver blocks from the "PCS 7 Library V6.0" are required in addition to the necessary hardware.

Definition

We speak of redundant switched I/O when there are multiple analog or digital I/O modules for a process signal and these can be addressed by both the primary and backup central processing units. I/O modules can be used either directly in the automation station, in expansion units or in a distributed I/O device, ET 200M for example.

Note

When non-redundant actuators/sensors are used, the inputs and outputs to and from the redundant modules have to be decoupled by means of terminal blocks with integrated diodes. Refer to the elementary circuit diagram for the respective board to determine if the diode decoupler is already integrated.

Configuration in HW Config and CFC

Two identical I/O modules can be configured for redundant operation via HW Config. Using CFC you then have to place a single channel driver block for each paired redundant signals and connect the signal with the lower address to the block in the same way you would for a non-redundant signal. The driver wizard handles the placement, connections and parameter settings of the driver blocks.

Further Topics

Manual Automation System S7 400H; Fault-Tolerant Systems

How to Configure Redundant I/O Modules

I/O Module Failure

STEP 7 online help

Simatic Process Control System PCS 7 Configuration Manual; Engineering System
2.1.9 **DP/PA-Link**

DP/PA-Link consists of the interface module IM 157 and one or more DP/PA couplers that are interconnected through the backplane bus.

The DP/PA coupler is a transceiver that interconnects PROFIBUS-DP and PROFIBUS-PA. It is a slave on the PROFIBUS-DP and master on the PROFIBUS-PA. Seen from the automation system, the DP/PA-Link is a modular slave. One or more couplers associated with the link provides PROFIBUS-PA networks to which field devices are connected.

Data can be transmitted to the automation system via PROFIBUS-DP at a maximum speed of 12 Mbaud. This is also currently the speed of the fastest connection between PROFIBUS-DP and PROFIBUS-PA and can be used by all DP masters with a DP interface.

The DP/PA-Link decouples a variety of baud rates in the bus system brings the lower-level PA devices together at one PROFIBUS-DP address. This makes it easier to communicate with PROFIBUS-DP masters.

Two IM 157 interface modules and corresponding bus modules are required in the bus module for connection to redundant PROFIBUS-DP. DP/PA couplers are required as transceivers. The connected PA nodes are single.
Physical Bus Characteristics

As a PROFIBUS physical layer for the processing industry, PROFIBUS-PA uses a transmission technology based on IEC 1158-2, in which the baud rate is specified as 31.25 Kbps. The application protocols for PROFIBUS-DP and PROFIBUS-PA are identical. The baud rate for PROFIBUS-DP is limited to 45.45 Kbps when a coupler is used without a link.

The DP/PA coupler can be used with a DP/PA link when higher baud rates are required. The DP/PA coupler can be operated with SIMATIC S5/S7 automation systems and all PROFIBUS-DP master that support the 45.45 Kbps baud rate. A maximum of 10 PA devices can be connected to a single DP/PA coupler. The actual number depends on the power consumption of the connected PA devices. The DP/PA coupler has to be installed in a safe area outside an area with danger of explosion. The connected PA cable can be laid in an area with danger of explosion and meets the explosion protection norm, EEx ia IIC.

Further Topics

Configuring DP/PA-Link

Manual DP/ PA-Link and Y-Link Bus Connections
2.1.10 Y-Link

Y-Link consists of two IM 157 interface modules and a Y coupler interconnected through the bus module. Y-Link creates a gateway from the redundant DP master system of an S7-400H to a non-redundant DP master system. This enables devices with only one PROFIBUS-DP interface to be connected to a redundant DP master system as switched I/O.

![Diagram of Y-Link configuration]

A standard rail with the corresponding bus modules (BM IM/IM and BM Y coupler) is used to configure the Y-Link.

The new generation of Y-Link no longer requires a repeater and is capable of forwarding diagnostics requests from the corresponding function modules or I/O modules to the CPU.

Beginning with SIMATIC PCS 7 Version 6.0, DP V1 backups can be connected downstream from the Y-Link in addition to the standard PROFIBUS-DP backups.

Further Topics

- Configuring Y-Link
- Manual DP/PA-Link and Y-Link Bus Connections
2.1.11 PROFIBUS Connection to the Automation Station

A PROFIBUS connector is required for connecting the PROFIBUS-DP connection to the CPU of the automation station. If you wish to use the plastic cover supplied for the CPU module, you will need a PROFIBUS connector with an angled cable outlet in short design.

Further Topics

Manual Diagnostics Repeater for PROFIBUS-DP

2.1.12 Redundant Actuators and Sensors

Actuators and sensors on the field-I/O level can be configured redundantly for PCS 7. Depending on the I/O module to which the redundant actuators or sensors are connected, failure of an actuator or sensor can be detected and reported to the control system as a fault. The system can perform a failover to the operational actuator/sensor when an actuator/sensor fails. This ensures that the current status of the process value can be read or displayed at any time.

Note

Please refer to the product documentation of the corresponding I/O module to determine if it supports detection and reporting of failures from connected actuators or sensors.

Further Topics

Manual Process Control System PCS 7 System Description
2.2 Solutions for Automation Systems

2.2.1 Solutions for Automation Systems

This chapter presents solutions that can be used to increase the availability of an automation system. Fault-tolerant automation system are often used when extremely fast reaction time is required for process errors, for example, when switching in milliseconds. With the fault-tolerant S7-400H automation system, SIMATIC PCS 7 enables you to configure your process control system with redundancy.

The S7-400H automation system and all the other components in the PCS 7 environment are finely matched.

This solution consists of two CPU’s where the second, standby CPU is synchronized to the events of the master CPU. The second CPU performs the same application processing steps as the master CPU. If the master CPU fails, the standby CPU continues the processing without interruption. We refer to this type of failover as "Hot standby".

There are always two central processing units and power supplies in an S7-400H. The communication processors and I/O modules are expansion modules.

2.2.2 S7-400H Hardware Components

The following hardware components are available for the configuration of a fault-tolerant automation system.

<table>
<thead>
<tr>
<th>Hardware Components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mounting rack UR2-H</td>
</tr>
<tr>
<td>Mounting rack UR2</td>
</tr>
<tr>
<td>Mounting rack UR1</td>
</tr>
<tr>
<td>Central processing unit CPU 414-4H</td>
</tr>
<tr>
<td>Central processing unit CPU 417-4H</td>
</tr>
<tr>
<td>Synchronization modules</td>
</tr>
<tr>
<td>Synchronization cable (length 1 m)</td>
</tr>
<tr>
<td>Communication processor CP 443 - 5 EXT</td>
</tr>
<tr>
<td>Communication processor CP 443 - 1</td>
</tr>
</tbody>
</table>
Mounting Racks

We recommend the UR2-H mounting rack for the configuration of the S7-400H. The mounting rack enables you to configure two separate subsystems, each containing nine slots, and is suitable for installation in 19" cabinets. The subsystems of this mounting rack are electrically, but not mechanically, isolated. It is therefore important to note when using this mounting rack that it cannot be replaced during online process operation. The complete system always has to be shut down first. You can also configure the S7-400H with two physically separate mounting racks. This allows its replacement during online operation. The mounting racks UR1 or UR2 can be used for such a configuration.

Central Processing Units

There are two CPU's (CPU 414-4H or CPU 417-4H) in a fault-tolerant system and they are interconnected through a synchronization module and fiber-optic cables.

Power Supply

A separate power supply module from the S7-400 system series is needed for each subsystem of the S7-400H. There are power supply modules for DC 24V nominal input voltage as well as for AC 120/230 V with output current of 4, 10 and 20 A. Two power supply modules can be used in each subsystem to increase the availability of the fault-tolerant system. Use the power supply module PS 407 10 A R for AC 120/230 V input and 10 A output for such a configuration.
Synchronization Modules

Synchronization modules are used to couple the two central processing units. They are installed in the automation station and interconnected with fiber-optic cable. Two synchronization modules are installed in each automation station. The rack number of the fault-tolerant CPU is also set on the synchronization modules. The same rack number needs to be entered in each synchronization module in the CPU. In addition to holding the threaded bolts which facilitate exchanging synchronization modules, the front plates of the synchronization modules are also used for switching the power voltage. This feature is needed to enable replacement of synchronization modules even when the CPU is supplied with power. The synchronization modules will not operate without the tightened front plates.

Fiber-optic Cables

The fiber-optic cables are connected to the synchronization modules and form the physical connection (redundancy coupling) between the two automation stations. The synchronization cables cannot be cross-connected. In addition to the standard lengths of 1, 2, and 10 meters, custom-made synchronization cables are available with lengths up to a maximum of 500 meters.

Communication Modules

A variety of communication modules from the SIMATIC product family for PCS 7 can be used for communication tasks.

Communication processors used in the mounting rack of the automation system are referred to as communication modules. Communication processors installed in PCs (OS clients, OS servers, ES) are PCI network cards.

The physical transmission medium depends on the range, resistance to interference and the baud rate. Industrial Ethernet using fiber-optic cables or triaxial or twisted-pair copper lines can be used for the communication between the automation system and the OS servers. PROFIBUS-DP with electrical or optical components is used for the communication from the automation system to the distributed I/O devices. Both the transmission media and the communication processors can be installed in redundant form, that is, always doubled. If the active communication component (CP, Bus) fails, the communication is automatically continued through the redundant connection.

In addition to the fault-tolerant communication between the automation system and the OS servers and between the automation system and distributed I/O, fault-tolerant communication between two standard CPU's and between two fault-tolerant CPU's plays an important role in the transmission of data. Existing fault-tolerant Industrial Ethernet can also be used. However, the additional fault-tolerant S7 connection parameters need to be configured in "NetPro". A variety of communication blocks are available in the PCS 7 library for the transmission of data (measured values, binary values, interlocks). The communication blocks differ in their transmission mechanism, which may be secured or unsecured, for example.
Further Topics
How to Insert a SIMATIC Fault-tolerant Station into Your Project
How to Insert Synchronization Modules into the Fault-tolerant CPU
How to Configure Redundant Communication Processors
Manual Automation System S7-400H; Fault-tolerant Systems

2.2.3 How the S7-400H Operates

The automation system consists of two redundantly configured subsystems, which are synchronized through fiber-optic cables. The two subsystems form a fault-tolerant automation system that operates with a dual-channel design according to the principle of active redundancy. Active redundancy, often referred to as functional redundancy, means that all redundant components are in continual operation and are simultaneously participating in the processing control tasks. The user programs loaded in both CPU’s are fully identical and are run synchronously by both CPU’s.

If the active CPU fails, the automation system automatically switches to the redundant CPU (414-4H, 417-4H). The failover has no effect on the ongoing process because it is bumpless.

Further Topics
Manual Automation System S7-400H; Fault-tolerant Systems
2.3 Solutions for Communication

2.3.1 Solutions for Communication

The availability of a process control system is not only determined by the automation system, the environment also plays a considerable role. In addition to the control and monitoring components, this especially includes a high-performance communication system that connects the management level (HMI) with the process control and the process level with the field-I/O level. Distributed control systems are also needed in manufacturing and processing automation. This means breaking down complex control tasks into smaller, simpler steps and distributing them within the system. This, in turn, increases the demand on the communication between the distributed systems. A high-performance, extensive communication system is needed to fulfill this demand.

This requirement is met by using redundancy in the communication connections between the components of the automation system.

Local networks (LAN) form the basis of the communication system. The following are options that can be implemented based on the specific system requirements:

- Electrical
- Optical
- Electrical/optical combination

Communication connections are organized in three bus groups (field bus, system bus and terminal bus). This chapter presents the redundancy concepts for these control engineering levels.
When a communication error occurs automatic failover is performed from the active connection to the backup connection. Both connections use the same medium and protocol. The failover has no effect on the user program running in the CPU.

Redundancy through an electrical or optical ring

A redundant ring structure can be configured with the following S7 network components:

- Terminal bus: Industrial Ethernet with electrical switch modules (ESM) and/or optical switch modules (OSM)
- System bus: Industrial Ethernet with electrical switch modules (ESM) and/or optical switch modules (OSM)
- Field bus: Optical PROFIBUS/OLM (optical link module)

All networking options of the modules listed above are capable of overcoming a broken cable at any location in the ring. The redundancy is provided by the link or switch modules, which automatically find an alternate path around the ring.

Connections

- OLM's offer connections for 3 PCs, connection types: twisted pair and industrial twisted pair
- ESM's and OSM's offer connections for 6 PCs, connection types: TP (twisted pair) and ITP (industrial twisted pair)

Electrical Ring

Redundant ring structure with ESM's. A "ITP XP Standard Cable 9/9" is used for all connection lines. ESM in RM mode (redundancy mode) is the module with the gray background in the illustration.

Optical Ring

An optical ring has to be configured with at least two optical link or switch modules. OLM's and OSM's cannot be operated together.
A converter is used when OSM's and ESM's are operated together. Optical modules are interconnected with fiber-optic cables. Fiber-optic cables with lengths up to 3 km can be connected to the optical connections. Long distance (LD) type modules are used for distances up to 26 km. Electrical network lines with TP or ITP connectors are used to connect the nodes to the optical modules. Redundant ring structure with OSM's. A "fiber-optic cable (FO)" is used for all connection lines. ESM in RM mode (redundancy mode) is the module with the gray background in the illustration.

Optical/Electrical Ring

An optical/electrical ring is a combination of both media. The medium transition from electrical to optical and vice versa is performed by converters (EMC=Electrical Media Converter, OMC=Optical Media Converter). Electrical connection can extend up to 6 meters, optical connection up to 26 km.

Further Topics

Manual SIMATIC Net Twisted Pair and Fiber Optic
Manual SIMATIC Net Industrial Ethernet OSM/ESM
Manual SIMATIC Net PROFBUS Networks
Manual SIMATIC Communication with SIMATIC
2.3.2 Redundant Field Bus

The field bus for data communications between the automation system and the distributed I/O is PROFIBUS, which is used as the standard field bus for manufacturing and process automation. PROFIBUS contains the specifications for the bus characteristics, the access methods for the user protocol and the user interface. The following PROFIBUS protocols can be used in the process or field communication:

- PROFIBUS-DP (distributed I/O) for fast, cyclic data communication with field devices. Used to connect distributed I/O, SIMATIC ET 200 for example, very fast response time.
- PROFIBUS-PA (process automation) for process automation applications and communication with intelligent field devices. Enhances PROFIBUS-DP with the addition of intrinsically safe transmission technology.

It is often advantageous to connect several PROFIBUS-DP lines to an automation system in order to increase the number of I/O components that can be connected. Segments can also be configured to enable individual production areas to operate independent of one another.

Note
The AS must be equipped with the CP 443-5 Extended communication processor and CP 443-1 to be able to address the field devices using the “Record Routing” function in the SIMATIC PDM software.

Optical PROFIBUS with Link Modules

Optical link modules (OLM's) enable the configuration of a redundant optical network in line, ring and star structures. The maximum distance between two OLM's is 15 km. The baud rate can be set in steps of 9.6 Kbps to 12 Mbaud.

The fiber-optic option of PROFIBUS has the following characteristics:

- Suitable for long distances
- Resistant to electromagnetic interference
- Electrical isolation
- Can use a variety of fiber-optic cables

Configuration Options

The following fault-tolerant communication solutions are offered for PROFIBUS-DP:

- Redundant PROFIBUS-DP as an electrical network
- Optical network with OLM's
Components

The fault-tolerant S7-400H automation system features a PROFIBUS-DP master interface on each CPU for connecting to PROFIBUS-DP. For switched distributed I/O, the connection to the I/O device is made through two IM 153-2 interface modules.

The following illustration shows an electrical network with PROFIBUS-DP.

Availability of the Redundant Field Bus

The communication from the sensor to the fault-tolerant system is carried out through the redundant bus connection when the active bus connection fails.
The system bus connects the automation systems with the OS servers and is operated as Industrial Ethernet with 10 or 100 Mbaud. The connection to a redundant system bus is made through Ethernet communication processors (CP's), which are installed in each subsystem of the automation system and in the OS servers.

When a redundant system bus is used and the active network connection fails, the communication between the automation system and the OS servers is switched to the second, redundant network connection. This ensures the availability of the network connection at all times.

Network connections between OS servers and fault-tolerant stations (AS) can be configured as electrical or optical. Redundant and single bus systems cannot be operated together.

For PCS 7 the system bus is usually configured as a redundant ring with OSM/ESM. Redundant OS servers are equipped with a CP 1613 and each subsystem in the fault-tolerant automation system is equipped with up to two CP 443-1.

An even higher level of availability can be achieved with PCS 7 by installing another redundant ring with OSM's/ESM's with two CP's per OS server. A block diagram of this system's components is provided in the section "Availability of the system bus as a redundant double ring".
Configuration Options

The following communication solutions are offered to increase the system availability:

- Redundant electrical or optical network with ESM's/OSM's operated as Industrial Ethernet with 10/100 Mbaud.
- Combination redundant network with OSM's, ESM's, fiber-optic and electrical connections with 100 Mbaud.
- Redundant connection of network segments with two OSM/ESM's. Here one OSM/ESM is connected as a standby slave and the other OSM/ESM operates as the standby master. The standby sync ports of both OSM/ESM are interconnected by a ITP XP standard cable 9/9. Such a connection is shown in the following illustration:

Components

The following illustration shows a redundant system bus in ring structure with OSM's. Note that this architecture could be created using ESM's as well.

In contrast to the redundant system bus with a ring structure shown above, a double redundant system bus with OSM's appears as follows. Note that this architecture could be created using ESM's as well.
Availability of the System Bus as a Redundant Ring

In this type of system one CP 443-1 may fail in each subsystem of the AS without it affecting the complete system. The system bus (marked with *) features OSM redundancy and can overcome a bus line broken at any location. One of the two OSM's to which the OS servers are connected may fail without it affecting the complete system. If one OSM fails, the redundant OS partner server can continue to communicate through the operational OSM. The same scenario applies to the OSM's, each of which is connected to a CP of a fault-tolerant subsystem.

A redundant double ring, described below, can be used to guard against failure of all the OSM's.
Availability of the System Bus as a Redundant Double Ring

The block diagram for a system bus configured as a redundant double ring, each with two CP's in the OS servers and additional OSM's/ESM's, appears as follows:
In this system a CP 1613 can fail in each OS server, or a CP 443-1 can fail in each subsystem of the AS without it affecting the complete system. There are two system busses (BUS) and each features redundant OSM's. This covers the failure of the BUS components including all of the participating components (OSM's/ESM's).

Further Topics

Configuring Redundant a System Bus

Manual SIMATIC Net Twisted Pair and Fiber Optic

Manual SIMATIC NET Industrial Ethernet OSM/ESM Network Management

Manual SIMATIC Communication with SIMATIC

2.3.4 Redundant Terminal Bus

The terminal bus connects the OS servers with the OS terminals (OS clients, ES). The terminal bus can be configured redundant with S7 network components. The redundancy capability of the terminal bus is guaranteed by the OLM's, ESM's and OSM's. For example, a broken cable in the connection between the modules is tolerated and the communication remains uninterrupted. This ensures the availability of the bus connection at all times.

If the terminal bus fails, no process data would be sent from the OS servers to the OS clients.

Configuration Options

The following solutions are offered to guard against failure of the terminal bus:

- Redundant ring structure in an electrical network with ESM's, 100 Mbaud. The connection to the ESM's is electrical.
- Redundant ring structure in an optical network with OSM's and fiber-optic cables, 100 Mbaud. The connection to the OSM's can be either electrical or optical (BC08 used together with a TP11 media converter).
- Redundant ring structure in a combination network with optical and electrical switch modules and fiber-optic cables, 100 Mbaud. The connection to the OSM's is electrical.

Components

In the following illustration the terminal bus is shown as a redundant ring with OSM's. The OS servers are connected to the OSM's in a distributed pattern in order to take optimal advantage of the OSM functionality. The failure of an OS server due to the failure of an OSM is reduced and the bus load is also reduced. The log data of the control process is secured and continuously available due to
the use of two OS clients each equipped with a line printer for printing the message sequence reports.

**Note**
When one of the OSM’s fails (see illustration above), all connected nodes fail as well. Redundant OS servers, therefore, should not be connected to the same OSM’s.

**Availability of the Redundant Terminal Bus**
Communication between OS clients and OS servers is guaranteed even if the optical ring line between the optical switch modules is broken. However, if one of the optical switch modules fails, the connection between the connected OS servers and the OS clients is interrupted. A redundant double ring is a solution to this problem.
Further Topics

Configuring a Redundant Terminal Bus

Manual SIMATIC Net Twisted Pair and Fiber Optic

Manual SIMATIC Net Industrial Ethernet OSM/ESM
2.4 Solutions for OS Servers

2.4.1 Redundant OS Servers

SIMATIC PCS 7 enables you to configure two OS servers redundantly for fault-tolerant operation. This ensures that you can monitor and control your control process at all times. The solution represents the entry level into fault-tolerant process control systems.

If one of the two OS server fails, the OS partner server takes over the process. The interface between OS clients and the automation system remains available. This solution ensures that no process data is lost due to the failover time or disruption of an OS server since the redundant OS partner server also archives the process data. The two OS servers synchronize themselves with the current process data when a failed OS server comes back online.

When one OS server in a redundant OS server pair fails, the internal master/standby identification changes from the failed OS server to the OS partner server. The master identification remains with the OS partner server even when the failed OS server comes back online.

Method of Operation

Redundant OS servers monitor each other during operation in order to detect the failure of an OS partner server as early as possible. When one of the two OS servers fails, the OS clients automatically switch to the redundant OS partner server. This means that the OS clients always remain available for the control and monitoring of the process. During downtime, the redundant OS partner server continues to archive all messages and process data in the WinCC project. Once the failed OS server comes back online, the contents of all the message, process value, and user archives are automatically copied to the returning OS server. This copy process is referred to as redundancy synchronization. Redundancy synchronization fills the gaps in the various archives that result from failures.

Tag logging and alarm logging have to be configured functionally identical for redundant OS servers. Functionally identical configuration means the same archives, whereby extensions in the form of additional measuring points and archives are permitted. Functionally identical configuration is ensured by configuring the OS partner servers (OS_Stby) in the SIMATIC Manager and then using the menu command "PLC" -> "Download".
Configuration

The following configuration shows how redundant OS servers basically work.

Note
With SIMATIC PCS 7 redundant OS servers must also be interconnected by a serial null modem cable. This connection provides a dedicated communication path for server-to-server data exchange.

Availability of Redundant OS Server Pairs

The availability of the complete system is ensured even when one of the two OS servers fails because the two OS servers form an independent redundancy node.

Note
The busses marked with * (terminal bus and system bus) can be configured redundantly with optical or electronic switch modules.
Further Topics

How to Configure an OS Server and Its Redundant OS Partner Server
WinCC online help; WinCC Redundancy

2.4.2 Time Synchronization

A process control system is synchronized when all of the individual components relying on the time have an identical date and identical time-of-day. A synchronized system time is highly important, especially for the PCS 7 redundancy features, such as the redundancy synchronization between redundant OS servers or BATCH servers. Synchronization of the OS server, the connected clients as well as the AS components is also a critical requirement for signal processing that needs to be performed in correct chronological order, such as archiving or message displays. The synchronization can only be used in process control systems with SIMATIC Industrial Ethernet bus systems.

The time generator can also be configured as a redundant component.

The SIMATIC WinCC “Time Synchronization” Editor is used to synchronized OS servers amongst themselves and the OS clients to the OS servers.

Windows Domain Synchronization

Synchronization is performed automatically within a Windows 2000 domain network by the Windows 2000 operating system. This Windows 2000 domain synchronization is an essential requirement for the authentication functions in a Windows 2000 domain.

When the synchronization through the terminal bus (LAN: Local Area Net) and through the system bus are both used, the time-of-day for a PC is always synchronized via the terminal bus.

The SNTP (Simple Network Time Protocol) is used for Windows domain synchronization. Since this only guarantees a clock precision of ±2 seconds and the standard synchronization interval is only every 8 hours, this synchronization scheme may be insufficient for runtime operation.

The following is a list of various scenarios:

1. Synchronization via the system bus (master/slave)

   Characteristic: The synchronization (master/slave) is performed exclusively via the system bus. No synchronization is carried out via the terminal bus.

   Application: Default setting for PCS 7 OS servers on the system bus. The PC is not a computer in a Windows 2000 domain.
2. Synchronization via LAN with a connected WinCC server (slave)

Characteristic: The synchronization is performed exclusively via the terminal bus. No synchronization is carried out via the system bus.

Application: Default setting for PCS 7 OS clients that are not connected to the system bus. The OS client has to have imported packages of at least one OS server connected to the system bus.

Synchronization of an OS server that does not have a connection to the system bus (e.g. an OS server that is only used as an archive server). The OS client has to have imported packages of at least one OS server connected to the system bus.

3. Synchronization via LAN with specifically defined computers (slave)

Characteristic: The synchronization is performed exclusively via the terminal bus. No synchronization is carried out via the system bus.

Application: Synchronization of an OS client that is not connected to the system bus. The time generator can be any PC using the Windows 2000 operating system.

Synchronization of an OS server that does not have a connection to the system bus (e.g. an OS server that is only used as an archive server). The time generator can be any PC using the Windows 2000 operating system.

Options: Time slave of a specifically defined PC

Time slave of two specifically defined PC’s. When PC 1 fails, there is an automatically failover to PC 2. PC 2 remains the time master until it experiences a failure.

Note: When PC 1 comes back online, there is no automatic master switchover back to PC 1 due to performance considerations.

4. Time slave on the terminal bus, time master on system busses

Characteristic: The PC reacts like a time slave on the terminal bus (LAN) and simultaneously a cooperative master on the system busses.

If one or both of the system busses are synchronized by other sources, the application switches the synchronization for the two devices to the standby mode. The PC clock, however, is not synchronized by the system bus even in this case. The PC clock is also not synchronized even when the computers PC\_name\_of\_first\_PDC and PC\_name\_of\_first\_PDC are not available! If there is no time master on either system bus, the application switches the synchronization on both devices to the master mode.

Application: The PC is in a W2K domain. PCS 7 OS is used as the time generator on the system bus. The time of day is taken from the Windows domain controller and forwarded via the system busses.

Options:

No additional time master on the system bus (e.g.: SICLOCK).
Additional time master on the system bus is used (e.g.: SICLOCK). Since two independent time masters are active on the terminal bus and system bus in this scenario, these have to be synchronized using a special method. This may involve using DCF77 or GPS time reception service, for example.

5. 3rd-party synchronization sets the system clock, time master on the system busses.

   Characteristic: The time of day on the PCs is set by a 3rd-party solution, i.e., there is no synchronization by the application. The synchronization is performed neither via the terminal bus nor the system bus.

   PCS 7 OS server is a cooperative master on the system busses. If one or both of the system busses are synchronized by other sources, the application switches the synchronization for the two devices to the standby mode. The PC clock, however, is not synchronized by the system bus even in this case.

   Application: The synchronization of the PC is carried out by a 3rd-party software component. Only the 3rd-party software is allowed to set the PC system clock.

   The PC is in a W2K domain. The synchronization of the PC network is performed exclusively by the internal Windows mechanism (SNTP).

   Note: This setting is only recommended for Windows 2000 domains when the SNTP synchronization can guarantee an acceptable time precision (+/-2 seconds within a site) for the OS clients. For PCS 7 (specified time precision ±10 ms), we recommend the setting described under point 4 instead.

   Special support is available for DCF-77 time reception service. The synchronization via the terminal bus must be deactivated and the control box "Use time reception service" must be set.
External Receiver

The following components are available for synchronization of the control system via an external receiver:

- GPS satellite receiver, connection via RS232 (COM port)
- DCF77 long wave receiver, connection via RS232 (COM port)
- Time generator SICLOCK, connection via system bus

In order to use the SIMATIC WinCC "Time Synchronization" Editor, one of the following communication processors has to be installed in the OS server that connects the process to the automation system.

<table>
<thead>
<tr>
<th>Communication Processor</th>
<th>Interface</th>
<th>Bus System</th>
<th>Used as time ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP 1613</td>
<td>PCI</td>
<td>Industrial Ethernet</td>
<td>Master and slave</td>
</tr>
</tbody>
</table>

The "DCF77 Reception Service" software, version > V1.18, is required to connect an external time receiver (GPS or DCF77) to an OS server.

Further Topics

- How to Synchronize the Time in Automation Systems to an External Time Generator
- How to Synchronize the Time in OS Servers to an External Time Generator
- How to Synchronize the Time on OS Clients to OS Servers
- Online Help WinCC; Time Synchronization
- Operating Instructions GPS Converter GPSDEC/GPSCOM
- Operating Instructions SICLOCK Time Transmitter
- Configuration Manual PCS 7 Process Control System, Operator Station
- Configuration Manual PCS 7 Process Control System
2.5 Solutions for SIMATIC BATCH

2.5.1 Redundant BATCH Servers

The SIMATIC PCS 7 process control system enables flexible automation of continuous and discontinuous processes, such as batch processes. Batch processes are carried out in the form of sequential or recipe controls. PCS 7 offers the SIMATIC BATCH V6.0 software package for batch processing. SIMATIC BATCH V6.0 helps you to control batch processes which demand compliance to standards and is especially suited to the PCS 7 process control system in regard to plant engineering and runtime functions.

SIMATIC BATCH V6.0 is a scalable product that serves as a cost-effective entry-level tool as well as a sophisticated high-performance tool to meet your growing needs. Both of the BATCH Engineering mechanisms in V5.3 and V4.02 are supported to facilitate software updating. SIMATIC BATCH V6.0 does not require dedicated hardware; it runs on the standard of SIMATIC PCS 7 components (AS, OS and ES) and any PC running SIMATIC BATCH V6.0 can be fully configured and loaded through the ES.

Redundancy Solutions with SIMATIC BATCH V6.0

SIMATIC BATCH V6.0 offers the following solutions using redundancy based on "hot standby":

- Data replication solution. With this solution each of the two redundant BATCH servers has its own database in which the BATCH data are stored. The two databases are continuously synchronized. This solution does not require additional hardware and software.

In the following illustration this redundancy solution is shown as an example configuration without PCS 7 OS.
Configuration - Replication Solution

Fault-tolerant replication solution

Redundant BATCH Server

Database synchronization

Fault-tolerant automation systems
Availability of Redundant BATCH Servers

The following two block diagrams of fully operational systems illustrates the fault tolerance of the BATCH clients and BATCH servers. All BATCH components form independent redundancy nodes since they are always doubled. This ensures the independence of the subsystem.

**Note**

Only the BATCH components and the terminal bus are shown in the block diagrams. The terminal bus marked with * can be installed redundantly with OSM's or ESM's.

The communication between BATCH clients and BATCH servers is carried out through the terminal bus.

The BATCH servers also communicate with OS servers through the terminal bus. The OS servers are connected to the automation system by the system bus.

**Further Topics**

- How to Configure a PC Station for a Redundant BATCH Server
- How to Configure a PC Station for a BATCH Client
- Manual and Online Help for SIMATIC BATCH
2.6 Solutions for OS Clients

2.6.1 Additional OS Clients

OS clients are PC stations that enable control and monitoring of an automation process. They are connected to OS servers through the terminal bus. OS servers function as HMI connections to the automation system.

An OS client has its own WinCC project and visualizes the process data generated on an OS server.

The failure of an OS client does not disturb the complete system because the automation program in the CPU continues to control the process and the OS servers continue to process and archive the process data. However, the visualization of the process is lost temporarily (for several seconds) and the process can only be influenced through the OS servers or other clients. Additional OS clients can therefore be integrated in your system to protect against failure.

By specifying a preferred server, several OS clients can be distributed equally amongst the redundant OS servers. The automation process can therefore be operated continuously, even during the failover from the active OS to its OS partner server.

Further Topics

How to Create an OS Client
WinCC online help

2.6.2 HMI Continuous Operation

"Continuous operation" in a redundant environment means the unrestricted ability to influence the system at any time even when confronted with the failure of one of the redundant OS servers. It is the most important safety characteristic for plants with critical operations.

This function is important for all customers who need to maintain continuous control over a process even though they can overcome the failure of an OS server in a redundant configuration. In the event of an OS server failure, all OS clients connected to the failed server will temporarily lose their connection to the process while they switch over. In order to ensure that continuous control and monitoring capability of the automation process is provided, the OS clients are distributed equally over the redundant OS servers by specifying a preferred OS server. The failure of some OS clients can then be tolerated because the remaining clients will continue to be connected to the process.

The expression "preferred server" refers to an OS server among the redundant OS server pairs which is given priority by OS clients when failover occurs. A preferred server can be defined separately for each OS client to guarantee continuous operations. The distribution of the OS clients over the OS servers also distributes the load and therefore increases the performance of the system as a whole.
Method of Operation

When the active OS server fails, the process values on all of the connected OS clients are no longer updated and operator input cannot be performed on these OS clients during the failover (this period typically lasts for several seconds). Other OS clients, which are connected in parallel to the redundant OS partner server, are not affected by this. The plant operator can therefore change to these OS clients if needed.

In general, the OS clients always switch to the specified preferred server when it is available. If it is not available, the OS clients automatically switch to its redundant OS partner server. If no preferred server has been specified for an OS client, it will connect to the OS server that has the master identification.

When the failed OS server comes online again, the OS client reconnects to its preferred server. The master identification of the OS server does not change even when the failed OS server comes back online.

Further Topics

How to Configure an OS client for Continuous Operation

WinCC online help

2.6.3 Engineering Station (ES)

The engineering station (ES) serves as a central configuration station. User programs, projects or OS clients, OS servers, AS components and the distributed I/O components are configured here. The configuration data is then transmitted from the ES to the destination systems (AS, OS, BATCH).

The ES is not typically used as a visualization station. It is therefore unnecessary to configure the ES redundantly.

Changes in the configuration data of project components such as AS, OS and BATCH are generally performed on the ES and then loaded on the destination systems. This makes PCS 7 configuration centralized and transparent.

Note

Engineering data not loaded on to the destination systems should be saved on external media to guard against data loss.
Configuration

The hardware (component configuration), networks and connections (NetPro) of a PC station ES are configured and loaded like a run-time OS, i.e. the ES becomes visible in NetPro.

The following points apply when "Named Connections", fixed configured connections, are used:

- When configuring the connections for the PC station ES, make sure that a connection is made for every AS. This will ensure that a connection can be established to every AS regardless of the WinCC project loaded.
- The connections from the individual PC stations (OS servers and ES) to the automation systems need to be named according to the following rule: all connections in an AS have to have the same name. Two connections need to be configured for each OS server and the ES, one in AS 1 and one in AS 2. The connections to AS 1 and the connections to AS 2 always must have the same name.
- Once this is accomplished, you can immediately test the WinCC project in the engineering station.

The Same Configuration for Redundant and Non-redundant OS Stations

The rule that fault-tolerant connections have to be configured in "NetPro", which was the case in versions up to SIMATIC PCS 7 V5.2, is no longer applicable. Redundant and non-redundant OS stations are now handled in the same manner.

System Changes in Online Operation

During the various system phases (commissioning, operation, maintenance), a variety of changes have to be made to the system and downloaded to the destination systems during online operation. This is performed in an incremental fashion with the "Download changes" command in SIMATIC Manager from an ES.
Multi-project Engineering

Multi-project engineering refers to configuration of several projects at once and is carried out using a high-level plant view in SIMATIC Manager. This plant view is created by a "Plant" object above the project level. In the component view the "Multi-project" hierarchy is added as a root, in other words, the projects are located below the multi-project level.

Component view

Plant view

Multi-project

Project 1

AS station 1

Project 2

AS station 2

Multi-project

Project 1

THQ 1

Same in both projects

Plant hierarchy object
Networks and Connections with Text References  The concept of text references for configuration of network connections is used in the ES. The text references are displayed in the connection list instead of the specification for the connection partner. A text reference is identical for both connection partners and defines the connection between the partners instead of the connection partner.

Agreement should be reached by the partners, however, to ensure that both parties use the same description.

- We differentiate between three connection configurations:
  A distributed configuration with subsequent conjunction.

- This allows you to navigate in projects beyond the currently selected project when selecting a connection partner. Once such a connection is established (S7-/H connection), future operations such as moving a connection partner into another project are kept consistent. This assumes that the connection partner is also available at this point in time.

- Connections are made in the multi-project context and then the projects are separated.
  The connections still remain consistent and convertible in this case. When you wish to edit such a connection, you receive the message that the connection partner is not available and, if you continue, the connection is broken and converted into a text reference.
### 3 Configuring Fault-tolerant Components

#### 3.1 Notes about Configuring Fault-tolerant Components

To ensure consistency in the configurations of the various fault-tolerant components presented here, the following requirements should be met:

1. Before beginning, you should make a chart or diagram containing all the network nodes and their network addresses.

2. When installing the hardware, ensure that all network nodes are cabled in an orderly manner. Star-shaped cabling is recommended for connecting the various types of high-performance and universally applicable communication terminals to workplaces. A modern cabling system should meet all of the currently effective laws, norms, standard recommendations and guidelines to provide you with the best advantages, in other words, flexibility, reliable features and a secure investment, both now and in the future. When you consider that such a cabling system will become part of the building infrastructure and the considerable expenses in installation, you should expect to get at least 10 years of use at maximum performance. This is the only way to rationalize and amortize such an investment. When dealing with large networks, complex environmental conditions and/or difficult user demands, such an infrastructure has to be accompanied by expert planning for future needs to offer investment protection.

3. In PCS 7 configurations all network nodes need to be assigned unique TCP/IP addresses, ISO addresses or PROFIBUS addresses.

4. When you are finished with the configuration in "HW Config" or "NetPro" you can use the "Save and Compile" command to check the consistency of your configuration. If the configuration contains an error, you will get a message containing information about the errors detected.

5. Of course, the necessary hardware has to be available and configured before you can download the configuration to the destination stations.

---

**Note**

The hardware is not mentioned in the requirements for the following configurations.

Refer to the documentation *SIMATIC PCS 7 Process Control System - Released PCS 7 Modules* for a list of released modules and firmware versions.
3.2  SIMATIC H Station

3.2.1  How to Insert a SIMATIC H Station into Your Project

The SIMATIC fault-tolerant station is contained in the hardware catalog of the "HW Config" configuration program in the SIMATIC Manager as a stand-alone type station. The configuration of two automation stations each with a fault-tolerant CPU and, therefore, a redundant process control system design can only be made with this type of station.

Requirements

- PCS 7 project

Configuration

1. Open your PCS 7 project in the SIMATIC Manager.
2. If you have not already done so, set the view in the SIMATIC Manager to component view using the "View" menu.
3. Select your project folder on the left side of the project window, open the context menu with a right mouse click and select "Insert new object". In the submenu that appears, click on "SIMATIC H Station".

Further Topics

Manual Automation System S7-400H; Fault-Tolerant Systems
3.2.2 How to Insert Synchronization Modules into the Fault-tolerant CPU

Similar to a SIMATIC 400 station, first the desired mounting rack such as UR2-H is inserted in the station by selecting the module from the catalog in HW Config in the station. This is then equipped like a standard station with a power supply or redundant power supplies, a communication processor or redundant CP's and the desired fault-tolerant CPU (414-4H or 417-4H). In the fault-tolerant CPU the sync modules have to be inserted in the slots "IF1" and "IF2".

Requirements

- Your PCS 7 project has to be open in the SIMATIC Manager.
- Mounting rack UR2-H has to be inserted twice in HW Config.
- In HW Config each mounting rack has to be equipped with a fault-tolerant CPU in slot 3.
- The "HW Config" configuration program has to be open.

Configuration

1. In "HW Config" click on the "View" menu and then click on "Catalog".
2. In the hardware catalog, double-click on the fault-tolerant CPU's you have inserted. Double-click on the version of your fault-tolerant CPU's in the structure that opens. The fault-tolerant synch module is located in the version folder, e.g., V3.0.
3. Select the fault-tolerant synch module, hold down the mouse button and drag it to the two slots "IF1" and "IF2" in both fault-tolerant CPU's.
Once the components have been inserted into the two subsystems of the fault-tolerant station, the configuration should appear in HW Config as follows:

Further Topics

Manual Automation System S7-400H; Fault-Tolerant Systems
3.2.3 How to Configure Redundant Communication Processors

Only Industrial Ethernet can be used as the system bus for a fault-tolerant system. In addition, the fault-tolerant system only supports the ISO protocol; it does not support TCP/IP. This limits the choice of Ethernet CP’s. Only ISO or multi-protocol CP’s can be used.

In a redundant system bus design, two CP’s are needed for each fault-tolerant subsystem.

Requirements

- Your PCS 7 project with a SIMATIC fault-tolerant station has to be open in the SIMATIC Manager.
- Mounting rack UR2-H has to be inserted twice in HW Config.
- In HW Config each mounting rack has to be equipped with a fault-tolerant CPU in slot 3 and the required sync modules.
- The "HW Config" configuration program has to be open.

Configuration

1. In "HW Config" click on the "Insert" menu and then click on "Hardware Components".
2. In the hardware catalog, double-click on the folder "SIMATIC 400". Then double-click on the folder "CP-400" and then on the folder "Industrial Ethernet".
3. Select the CP you are using, hold down the mouse button and drag it to a free slot in the mounting rack.

Note

When using a multi protocol communication processor make sure that the option "IP protocol is being used " in the dialog window "Properties - Ethernet Interface CP 443-1" under the "Parameters" tab is deactivated.
The configuration in HW Config should appear as follows:

Further Topics

Manual Automation System S7-400H; Fault-Tolerant Systems
3.2.4 How to Synchronize the Time in Automation Systems

Two dialogs must be configured in order to synchronize the time in automation systems.

Requirements

- Two communication processors, e.g., CP 443-1 Industrial Ethernet, installed and configured in the mounting rack.
- An external time source, e.g., a DCF77 long-wave receiver or GPSDEC satellite receiver, integrated in the Industrial Ethernet.
- Your PCS 7 project has to be open in the SIMATIC Manager.

Configuration in the dialog window "Properties - CPU ..."

1. In the left project window click on the automation system you are using, e.g., a SIMATIC fault-tolerant station. In the right window double-click on "Hardware" to open the selected station in "HW Config".

2. Open the context menu by right clicking on the CPU in slot 3 in the mounting rack, then click on menu item "Object Properties". In the "Properties - CPU ..." dialog window that opens select the "Diagnostics / Clock" tab.

3. In the clock section select "As slave" in the synchronization mode field to set the synchronization in the automation system. This means that the automation system receives its time from an external master time source.

4. Close the dialog window with the "OK" button.
Once you have completed these steps, the "Time-of-day synchronization" dialog should appear as follows:

Configuration in the dialog window "Properties - CP ..."

1. In the left project window click on the automation system you are using, e.g., a SIMATIC fault-tolerant station. In the right window double-click on "Hardware" to open the selected station in "HW Config".

2. Open the context menu by right clicking on the first CP used in a slot in the mounting rack, then click on menu item "Object Properties". In the "Properties - CP ..." dialog window that opens select the "Options" tab.

3. In the section for the time-of-day synchronization, activate the control box "Time-of-day synchronization".

   When there are several CP's in a station that are connected to the same bus, only one of these CP's should be permitted to pass time-of-day messages.

4. Close the dialog window with the "OK" button.
Once you have completed these steps, the "Time-of-day synchronization" dialog should appear as follows:

![Properties - CP 443-1 - (R0/SS)](image)

**Further Topics**

STEP 7 online help
3.3 Configuring Communication Connections

Once you have inserted all of the components (AS, OS and ES) in your project, you can configure the network connections between the SIMATIC components using "NetPro". When the configuration of the connections and network is completed, the configuration needs to be compiled, saved and downloaded to the CPU of the automation system.

Connection configuration can also be downloaded to the CPU even when the CPU of an AS is not in the "STOP" mode. To do this, select the connection to be downloaded in "NetPro" and use the menu command "PLC" > "Download" > "Selected Connections". It is not possible to connect to the processes on the operator stations until the connections are made known to the AS.

MAC addresses are always configured through "NetPro" in the properties dialog of the individual operator stations. The configuration has to be recompiled in NetPro each time it is changed.

When the network configuration, for example for a SIMATIC PC station, is saved and compiled, the system data and a configuration file (*.xdb file) is generated in the SIMATIC Manager. This data is only needed when there is no network connection to the destination system (runtime OS) and the configuration data therefore cannot be loaded from "NetPro". In this case the generated XDB file can be saved on a data carrier and brought to the destination system. There it can be manually imported by the station manager.

Further Topics
- How to Configure a Redundant Field Bus
- How to Configure a Redundant System Bus
- How to Configure a Redundant Terminal Bus

3.3.1 How to Configure a Redundant Field Bus

Communication connections are configured with the "NetPro" program in the SIMATIC Manager. PROFIBUS-DP is usually used as the field bus. The field bus connects the automation system to distributed I/O devices, ET 200M for example. A redundant field bus can only be created as part of a fault-tolerant system. One reason is that the CPU's of both subsystems only have one PROFIBUS-DP master interface; another reason is that when a subsystem fails, the remaining subsystem takes over the entire process and the communication to the distributed I/O device. In addition to the DP master interface, you can also use additional CP's, e.g., CP 443-5ext, in separate mounting racks for communication with intelligent field devices. Intelligent field devices are configured in the SIMATIC PDM (Process Device Manager). The DP master interface on the CPU module cannot be used for configuration of intelligent field devices via PDM's routing mode.
Requirements

- Your PCS 7 project with a SIMATIC fault-tolerant station has to be open in the SIMATIC Manager.
- Two 443-5ext type CP's have to be available in each subsystem of the fault-tolerant station.

Configuration

1. In the SIMATIC Manager open the "NetPro" program by selecting the menu command "Options" > "Configure network".
2. Open the hardware catalog by selecting the menu command "Insert" > "Network objects".
3. In the hardware catalog, open the submenu for subnetworks by clicking on the plus sign. Double-click on the PROFIBUS subnetwork to insert it into the network display.
4. Click on the "DP" square in the left subsystem of the SIMATIC fault-tolerant station and, holding down the mouse button, move the mouse vertically to the first PROFIBUS network. Repeat steps 3 and 4 for the right subsystem of the SIMATIC fault-tolerant station.
The completed configuration in "NetPro" should appear as follows:

The MPI connection (multi-point Interface) in the illustration is automatically inserted by "NetPro". It is used for the communication between such objects as programming devices (PG) and the AS. To create the connection paths for both subsystems, click on the square in "MPI/DP" of each subsystem and, holding down the mouse button, connect the interfaces to the MPI bus.

Further Topics

STEP 7 online help
3.3.2 How to Configure a Redundant System Bus

Communication connections are configured with the "NetPro" program. Industrial Ethernet is used as the system bus. The system bus connects OS servers to the automation system.

To configure a double redundant system bus with ESM's/OSM's, two CP's have to be physically present in each OS server and in each fault-tolerant subsystem, and they must be configured in NetPro. Two networks also must be configured in NetPro.

When a redundant ring with ESM's/OSM's is used, one network is sufficient for a redundant configuration. The use of additional CP's in the OS servers and in each subsystem of the automation system is determined by the degree of availability you desire. The procedures below describe a redundant ring with OSM's and without additional CP's.

Requirements

- Your PCS 7 project with a SIMATIC fault-tolerant station has to be open in the SIMATIC Manager.
- One 443-1 type CP has to be available in each fault-tolerant subsystem.
- Two SIMATIC PC stations each equipped with a type "1613" CP have to be inserted in your PCS 7 project.

Configuration

1. In the SIMATIC Manager open the "NetPro" program by selecting the menu command "Options" > "Configure network".
2. Open the hardware catalog by selecting the menu command "Insert" > "Network objects".
3. In the hardware catalog, open the submenu for subnetworks by clicking on the plus sign. Double-click on the Industrial Ethernet subnetwork to insert it into the network display.

   Note:
   To drag subnetworks into the NetPro project window, click on the network, hold down the left mouse button and drag it to the desired location. If you cannot place the object where you want it, you may need to move other objects to have the necessary space.

4. Click on the square in "CP 443-1" of the left subsystem and connect the interface with an Industrial Ethernet subnetwork. Repeat the procedure for the CP of the right subsystem.
5. Follow the same procedure for the CP's in both OS servers.
6. Save your configuration.
You should see the following configuration:

Further Topics

STEP 7 online help
### 3.3.3 How to Configure a Redundant Terminal Bus

The "NetPro" and "HW Config" programs do not support configuration of the terminal bus. SIMATIC NET offers several solutions for a redundant terminal bus. Redundant rings can be installed using OLM's, OSM's and ESM's.

### Further Topics

Visit the following Internet address to find more information about the individual SIMATIC NET products: [http://www.siemens.com/automation/service&support](http://www.siemens.com/automation/service&support).

Click on "Product Support". In the left navigation window click on "Automation Systems" and then on "Overview". In the right window click on "More Info" and the "Manuals". Now click on "To Manual Search". You can enter a search term and click on the "Search" button. Enter a keyword such as "OSM or ESM". The following manual should be included in those offered for downloading.

- Manual *SIMATIC Net Twisted Pair and Fiber Optic*
- Manual *SIMATIC Net Industrial Ethernet OSM/ESM*
- Manual *SIMATIC Net PROFIBUS Networks*
3.4  Distributed I/O

3.4.1  How to Configure the Redundant IM 153-2 Interface Module for an ET 200M I/O Device

The IM 153-2 interface module enables the configuration of redundant PROFIBUS-DP systems. If the active interface module fails, there is a bumpless failover to the backup IM 153-2 which takes over the intended functions. The active interface is indicated by an illuminated “ACT” LED on the IM 153-2. Two IM 153-2 are mounted on the bus module of the ET 200M for redundant operation.

Once you have integrated the IM 153-2 interface modules as hardware in the distributed I/O device, the component is made known to the system using "HW Config" or "NetPro" in SIMATIC Manager.

Requirements

- PCS 7 project with a SIMATIC fault-tolerant station and a configured DP master system

Configuration

1. Open your existing PCS 7 project in the SIMATIC Manager.
2. Select the SIMATIC fault-tolerant station in the left project window, open the context menu by clicking on "Open object" with the right mouse button. HW Config then opens.
3. Open the hardware catalog using the menu command "View" > "Catalog". In the "PCS7_V60_en" profile double-click on "PROFIBUS-DP" and then double-click on "ET 200M". Now select the IM 153-2 interface module, which is described in the hardware catalog text as "Interface module with active backplane bus".
4. Holding down the mouse button, drag the interface module IM 153-2 to one of the two PROFIBUS-DP segments and then release the mouse button.
5. In the "Properties – PROFIBUS Interface IM 153-2" dialog window that opens enter the PROFIBUS address and click on the "OK" button.
Configuration display in "HW Config"

Further Topics

Manual 10 ms Time Stamp

Manual Bus Connection Y-Link, Product Version 1
3.4.2 How to Configure Redundant I/O Modules

Signals from redundant I/O modules can be processed in user programs by function blocks. The signals are read and written through the process image to different addresses. In the user program the signals can be addressed fully transparent, whereby the lower address of the signal pair is always taken to be the master signal.

HW Config is used to configure the redundant I/O modules.

Only identical I/O modules (with the same order number) in analog or digital design can be used. The matching redundant modules are selected from the configuration and, once selected, are automatically associated together on a module-by-module basis. The following configurations can be made with redundant I/O modules:

- Redundant I/O modules in central and expansion devices
- Redundant I/O modules in non-redundant distributed I/O
- Redundant I/O modules in switched distributed I/O

Note

Redundant operation is possible only with certain modules from the S7-400 and ET200 M series. You will find a list of appropriate modules from both the S7-400 series and the ET200 M series in the manual, Automation System S7 400H; Fault Tolerant Systems.
Configuration Diagram

The illustration below shows an architecture with redundant input modules utilizing the distributed I/O family.

Method of Operation

"Signal Module 1" is configured as being redundant with "Redundant Signal Module 1". Individual channels, such as E1.1 and E10.1, are then automatically associated together.

Now if an error is detected in "Signal Module 1", "Signal Module 1" is disabled and only the signals from the redundant "Signal Module 1" are processed. The user program, therefore, still operates with the address E1.1, but the signal is coming from E10.1. The user program does not see an error since the signal status is still correct. A diagnostics message is generated by the module that has been disabled.
Configuring Fault-tolerant Components

Requirements

- A PCS 7 project with a fault-tolerant CPU (414-4 H/417-4 H, firmware 3.1) has to be available and open in the SIMATIC Manager.
- Two DP master systems have to be configured in each automation station.
- Two ET 200M, each with two IM 153-2 interface modules, have to be connected to the DP master system.

Configuration

1. In the left window section of the SIMATIC Manager double-click on the SIMATIC fault-tolerant station and then on "Hardware" in the right window section to open HW Config.
2. In HW Config select the first ET 200M (IM 153-2, redundant). The module overview is then displayed in the lower window section.
3. Open the hardware catalog and select an analog input module that supports redundancy. Holding the mouse button down, drag the selected module to a free slot in the ET 200M (lower window section) and then release the mouse button.
4. Repeat the procedure for the second ET 200M (IM153-2, redundant).
5. Select the first ET 200M again and then open the "Properties ..." dialog window for this input module by double-clicking on the inserted analog input module in the module overview. Then click on the "Redundancy" tab.
6. In the "Redundancy" tab window, select the option "2 modules" in the pull-down list for "Redundancy".
7. In the "Find Redundant Module" dialog that opens select a redundant module. Once you have selected the appropriate subsystem, the corresponding PROFIBUS address and the slot of the redundant module, all of the compatible modules in this subsystem are listed for selection. Select a module and then close the dialog with the "OK" button.
8. In the area for additional parameters you can enter additional settings for input modules. Close the dialog window with the "OK" button.

Further Topics

- STEP 7 online help
- Connecting Redundant I/O in the manual Automation System S7-400H; Fault-Tolerant Systems
3.4.3 How to Configure the Y-Link

Y-Link consists of two IM 157 interface modules and a Y coupler. The latest generation of Y-Link is capable of passing diagnostic information. Y-Link creates a gateway from the redundant DP master system to a non-redundant DP master system. This enables devices with only one PROFIBUS-DP interface to be connected to a redundant DP master system as switched distributed I/O.

Requirements

The following is required for configuration of a Y-Link:

- PCS 7 project with a SIMATIC fault-tolerant station and a configured DP master system

Configuration

The following configuration can be made with a Y-Link.
Configuration

1. Open your existing PCS 7 project in the SIMATIC Manager.

2. Select the SIMATIC fault-tolerant station in the left project window, open the context menu by clicking on "Open object" with the right mouse button. HW Config then opens.

3. Open the hardware catalog using the menu command "View" > "Catalog". In the "PCS7_V60_en" profile double-click on "PROFIBUS-DP" and then double-click on "DP/PA-Link". Now select the IM 157 interface module, which is described in the hardware catalog text as "Y-Link".

4. Holding down the mouse button, drag the IM 157 interface module to one of the two PROFIBUS-DP segments and then release the mouse button.

5. In the "Properties – PROFIBUS Interface IM 157" dialog window that opens enter the PROFIBUS address and click on the "OK" button. In the "Define Master System" dialog, click on "Interface Module for PROFIBUS-DP".
Configuration display in "HW Config"

Further Topics

Manual DP/ PA-Link and Y-Link Bus Connections
3.4.4 How to Configure the DP/PA-Link

DP/PA-Link consists of two IM 157 interface modules and one or more DP/PA couplers. The DP/PA coupler is used to build a gateway between a redundant PROFIBUS-DP subnetwork and a non-redundant PROFIBUS-PA subnetwork. In "HW Config" in the SIMATIC Manager only the IM 157 interface modules can be selected, the DP/PA coupler cannot.

The DP/PA coupler is transparent in regard to the addressing and the communication, i.e., it does not have its own bus address and it simply forwards the messages. The field devices connected to the PROFIBUS-PA are addressed directly by the CPU. The PA cable connected to the DP/PA coupler can be operated in Ex zone 1. The DP/PA coupler itself is accessory equipment and has to be installed in a safe area outside an area with danger of explosion.

The DP/PA coupler can be reconfigured during operation but it cannot be replaced. A list of PA backups that can be connected is available in the Y-Link manual. Please note that PCS 7 driver blocks are not available for all of the devices listed. Contact the PCS 7 Support Center to check if such a driver block is available for the device you have selected.

Requirements

The following is required for configuration of a DP/PA coupler:

- PCS 7 project with a SIMATIC fault-tolerant station and a configured DP master system
Configuration

The DP/PA coupler does not appear in the hardware catalog for the configuration of the bus system. You need to set the transmission speed of 45.45 Kbaud for the selected DP network in the "Properties PROFIBUS" dialog window under the "Network Settings" tab for the configuration in HW Config.
Configuration display in "HW Config"

Further Topics

Manual SIMATIC Bus Connections DP/ PA-Link and Y-Link
3.4.5 How to Import GSD Files

GSD files contain up-to-date device data that can be imported into the hardware catalog in HW Config. Device data from third-party manufacturers can also be imported in the hardware catalog. Once imported, the devices are available in the SIMATIC PCS 7 default profile and can be used in "HW Config".

---

**Note**
The procedures described here involving HW Config only apply for "Integrated SIMATIC PDM".

---

**SIMATIC PDM (Process Device Manager)**

In addition to the "Integrated SIMATIC PDM " option described here, SIMATIC PDM is also available as a stand-alone software package for configuration, parameterization, commissioning, diagnostics and maintenance of intelligent process devices (e.g., transducers) and for the configuration of networks.

SIMATIC PDM allows monitoring of process values, interrupts and status information of the device.

SIMATIC PDM does not require a STEP 7 installation and is fully operational without it. SIMATIC PDM does not use HW Config, the hardware configuration program in STEP 7, for example. The SIMATIC programs such as the SIMATIC Manager that are still needed, are included in the SIMATIC PDM package.

---

**Installation of the *.GSD Files**

1. The required GSD is installed in "HW Config" using the menu command "Options" > "Install New GSD...".
2. Open the "Options" menu and click on "Catalog". In the hardware catalog, set the "Default" profile.
3. Select the imported device under "PROFIBUS-DP" > "Other field devices" and drag it to the bus where you want it located.

---

**Note**
Those currently available transducers with PA connection are listed in the GSD file for the IM 157 interface module. Using the GSD file and a PROFIBUS-DP configuration tool, the DP/PA coupler can be configured for PROFIBUS-DP master. The GSD file can be downloaded without charge from the following Internet address: http://www.ad.siemens.de/csi_e/gsd.
3.5 SIMATIC PC Stations

3.5.1 How to Configure an OS Server and Its Redundant OS Partner Server

OS servers are connected to the automation system by the system bus. These PCs are equipped with 1613 type communication processors and form the process connection to the AS. OS servers are operated with Windows server operating systems and the software SIMATIC WinCC. SIMATIC WinCC is used to control and monitor the automation process. When the WinCC "Multi-user Project" type is created on the OS server, OS clients are able to connect to the OS server and visualize its process data.

PCS 7 allows you to configure an OS server and its redundant OS partner server in order to increase the availability of your process control system.

The following describes the individual steps involved in configuring the OS server and its redundant OS partner server.

Requirements

- STEP 7 project with a SIMATIC fault-tolerant station
- Your PCS 7 project has to be open in the SIMATIC Manager.

Configuration

1. If you have not already done so, set the view in the SIMATIC Manager to component view using the "View" menu.

2. Select your top project folder on the left side of the project window, open the context menu with a right mouse click and select "Insert new object". In the submenu, click on "SIMATIC PC Station".

3. Click the right mouse button on the SIMATIC PC station and then select "Object Properties". In the dialog window "Properties - SIMATIC PC Station", enter the desired name for the PC station. Close the dialog.

4. Double-click on the inserted PC station in the left project window. In the right project window, double-click on the "Configuration" component to open HW Config.

5. In the "Insert" menu, click on "Hardware Components". The hardware catalog opens. Click on the plus sign in front of the "SIMATIC PC Station" folder to open its submenu. Click on the plus sign in front of "HMI" and then on WinCC application. Holding down the mouse button, drag the component to the first slot of the OS server.

   In the hardware catalog, click on the plus sign in front of the folder "CP Industrial Ethernet" and then on the CP 1613 to place the CP in the second slot of the OS server. In the "Properties - ..." dialog that opens activate the control box "Set MAC Address / ..." and then click on "OK". Repeat this step for the second redundant CP.
6. Save your current settings, close the hardware catalog and go to the SIMATIC Manager.

7. Select your top project folder on the left side of the project window, open the context menu with a right mouse click and select “Insert new object”. In the submenu, click on “SIMATIC PC Station”.

8. Double-click on the inserted PC station in the left project window. In the right project window, double-click on the “Configuration” component to open HW Config.

9. In the “Insert” menu, click on “Hardware Components”. The hardware catalog opens. Click on the plus sign in front of the “SIMATIC PC Station” folder to open its submenu. Click on the plus sign in front of “HMI” and then on WinCC application (stby). Holding down the mouse button, drag the component to the first slot of the OS server.

   In the hardware catalog, click on the plus sign in front of the folder “CP Industrial Ethernet” and then on the CP 1613 to place the CP in the second slot of the OS server. In the “Properties - ...” dialog, activate the control box “Set MAC Address / ...” and then click on “OK”. Repeat this step for the second redundant CP.

10. Save your current settings. Close the hardware catalog and HW Config.

Your project should now look like the one in the following illustration. You can rename the components any way you please.

Further Topics

STEP 7 online help
3.5.2 How to Set the Project Paths of the Destination OS and Standby OS

To enable the OS and standby OS to detect one another, you must configure them so that they know the location of their partner's project.

Requirements

- Your PCS 7 project has to be open in the SIMATIC Manager.
- Two SIMATIC PC stations have to be configured as an OS server and OS partner server.

Configuration

1. Open the object properties of the OS server and set the project path to the OS server in the "Target OS and Standby OS" tab under "Path to the Target OS Computer". This is the path to the PC where the PCS 7 project will later be loaded. Either the target computer is already accessible in the network and you can select it or you have to edit the path to the computer.

2. Under "Standby OS" select the redundant OS partner server. The configured OS partner server is listed in the selection menu. The name of the redundant OS partner server is automatically renamed as "Master OS Name_StBy".

3. Close the object properties.

4. Open the object properties of the OS partner server and set the project path to the OS partner server in the "Target OS and Standby OS" tab under "Path to the Target OS Computer". This is the path to the PC where the PCS 7 project will later be loaded. Either the target computer is already accessible in the network and you can select it using the "Browse" button, or you have to edit the path to the computer.

5. Close the object properties.

Further Topics

STEP 7 online help
3.5.3 **How to Configure a Redundant Connection Between an OS and AS**

To complete the configuration of the OS server and its redundant OS partner server, you need to create the fault-tolerant network connections to the AS in "NetPro".

**Requirements**

- Your PCS 7 project has to be open in the SIMATIC Manager.
- Two SIMATIC PC stations have to be configured as an OS server and OS partner server and each has to be equipped with two type 1613 CP's.
- A redundant system bus has to be configured.

**Configuration**

1. Open the "NetPro" program with the menu command "Options" > "Configure Network".
2. In "NetPro", click on the first CP 1613 of the OS server and connect it with the "Ethernet(2)". Connect the second CP of the OS server to "Ethernet(1)".
3. The two CP's of the OS partner server are connected in the same way with the two Ethernet networks.
4. Select the WinCC application of the OS server in which you want to configure a fault-tolerant network connection. The connection table is displayed in the lower window section.
5. Position the cursor in the first free line of the connection table and select the menu command "Insert" > "New Connection". The "New Connection" dialog field opens.
6. Select the desired connection partner in the tree.
7. In the connection field, select the type of connection for the communication.
8. Activate the control box "Display properties before inserting". This allows you to make settings or changes to the connection.
9. Click on the "OK" button to save your settings.
The redundant network connection of the two fault-tolerant station OS servers should appear in NetPro as follows:

Further Topics

- Configuring a Redundant System Bus

STEP 7 online help
3.5.4 How to Assign an S7 Program to an OS

The "Compile OS" assistant is used to transfer AS data such as S7 programs, tags, messages and SFC charts to a destination OS. This procedure is necessary to be able to make all of the AS data accessible to an OS server.

Requirements

- Completed and tested S7 program
- "Named connections" has to be selected as the connection type for transferring to a fault-tolerant CPU.

Note

Only one transfer can be performed at a time!

Configuration

1. In the SIMATIC Manager start the "Compile OS" wizard by selecting the menu command "Options" > "OS" > "Compile".
2. Follow the instructions and information provided by the wizard.

Further Topics

STEP 7 online help
3.5.5 How to Configure WinCC Redundancy

WinCC Redundancy is used to implement redundancy between an OS server and its OS partner server. To begin, WinCC Redundancy has to be configured in the WinCC Explorer on the OS server.

Note
Be aware that only one of the two OS servers can be the "default master" and both of the OS servers cannot be activate with this option in the "Redundancy" dialog window. Problems may otherwise occur during failover of the OS client.

Requirements
- Your PCS 7 project has to be open in the SIMATIC Manager.
- Two SIMATIC PC stations have to be configured as an OS server and OS partner server and each has to be equipped with two type 1613 CP's.
- Serial connection between the two OS servers using an RS232 cable (null-modem cable) via a COM port.

Configuration
1. In the left project window of the SIMATIC Manager click on the OS in the OS server with the right mouse button. Select "Open Object" in the context menu. The WinCC Explorer opens.
2. In the WinCC Explorer click on the "Redundancy" editor with the right mouse button and then select "Open" in the context menu to start the "Redundancy" application.
3. In the "General" tab activate the "Default Master" control box if you want to set the current OS server as the default master.
4. In the "Redundant Partner Server" field enter the computer name of the redundant OS server. You can also use the "Browse" button to select an appropriate server from the network.
5. Activate the following control boxes as required:
   Synchronization of Tag Logging after the partner server comes back online
   Synchronization of Alarm Logging after the partner server comes back online
   Online synchronization for Alarm Logging
   Synchronization after process connection error
   Multi-client switch in case of a process connection error
   Select the COM port for the serial connection to the redundant partner
For more information about the "General" and "User Archive" tabs refer to the online help for WinCC.
6. Activate the control box "Activate redundancy".
7. Close the dialog window with the "OK" button.
The dialog in the "General" tab may be configured as follows:

![Redundancy Configuration Dialog](image)

**Optional Settings**

- Synchronization of Tag Logging after the partner server comes back online
- Synchronization of Alarm Logging after the partner server comes back online
- Online synchronization for Alarm Logging
- Synchronization after process connection error (Tag + Alarm Logging)
- WinCC client switch in case of a process connection error

Serial Verbindung zum redundanten Partner: COM1

Activates the synchronization of all specified options and the User Archives:

- Activate Redundancy

**Further Topics**

WinCC online help
3.5.6 How to Download a SIMATIC PCS 7 Project to PLCs

A PCS 7 project and its components (AS, OS, BATCH Server/Client) can be downloaded in a single procedure to the various destination systems using the SIMATIC Manager menu command "PLC" > "Compile/Download Programs".

You can also download the various components individually to the destination systems using the menu command "PLC" > "Download".

Requirements

- All of the required SIMATIC PC stations have to be configured in the SIMATIC Manager.
- The OS's have to be assigned as master and standby.
- The paths from the ES to the individual destination systems have to be set.
- The AS has to be configured with all of its components (synchronization modules, CP's, etc.).
- All network connections have to be configured, saved and compiled in "NetPro".
- The destination computer has to be equipped with an operating system, a network connection and WinCC.
- The SIMATIC Manager has to be open.

Configuration

1. Select your project in the left side of the project window of the SIMATIC Manager. Click on "PLC" menu and select "Compile/Download Programs" to compile all of the project components and download them to the destination systems.

Further Topics

STEP 7 online help
3.5.7 How to Configure an OS Client

OS clients are connected to OS servers by the terminal bus. OS client PCs can be integrated in the terminal bus using standard, commercially available Ethernet network cards. The terminal bus can be an electrical or optical design. OS clients visualize the process data in OS servers.

PCS 7 allows you to integrate, for example, two OS clients in your process control system and to connect them to a redundant pair of OS servers. This increases the fault tolerance in your process control system by offering failover to an OS partner server to ensure that the process data remains available to the OS client even when one of the two OS servers fails.

Requirements

• Your PCS 7 project has to be open in the SIMATIC Manager.

Configuration

1. If you have not already done so, set the view in the SIMATIC Manager to component view using the "View" menu.
2. Select your top project folder on the left side of the project window, open the context menu with a right mouse click and select "Insert new object". In the submenu, click on "SIMATIC PC Station". Repeat this step to insert another SIMATIC PC station.
3. Right click on the inserted SIMATIC PC station and then on "Rename" to assign a name of your choice to the PC station. Repeat this step for the second PC station.
4. Double-click on the inserted PC station in the left project window. In the right project window, double-click on the "Configuration" components to open HW Config.
5. In the "Insert" menu, click on "Hardware Components". The hardware catalog opens. Click on the plus sign in front of the "SIMATIC PC Station" folder to open its submenu. Click on the plus sign in front of "HMI" and then on "WinCC Application Client". Holding down the mouse button, drag the component to the first slot of the PC station.
6. Save your current settings and close the hardware catalog.
7. Repeat steps 5 and 6 for the second PC station.
Your project should now look like the one in the following illustration. You can rename the components any way you please.

Further Topics

WinCC Client
3.5.8 How to Configure an OS Client for Continuous Operations

To visualize the process data of an OS server, an OS client needs a "package of the OS server", in order to display its process data. Packages are generated on the OS servers and downloaded to the respective OS clients. This makes data relating to the configuration such as images, tags, messages and archives available to the OS clients.

A minimum of two OS clients are required to ensure continuous operations. A separate preferred server is specified for each client, distributing the OS clients to the redundant OS servers. This ensures that the process is continuously available even during the failover from one OS server to the redundant OS partner server.

Requirements

- A redundant OS server pair has to be configured in the SIMATIC Manager on the ES.
- WinCC Redundancy has to be configured on the ES for both OS servers.
- A package has to be generated on the ES for the OS Server (master).
- Two OS clients have to be configured in the SIMATIC Manager on the ES.
- The generated packages have to be downloaded from the ES to both OS clients on the OS server (master).

Configuration

1. Open the WinCC project of the first OS client in the component view of the SIMATIC Manager.
2. In the WinCC Explorer click on the project navigation window with the right mouse button and then on the "Server Data" editor and finally on "Configure".
3. In the "Configure Server Data" dialog window, click on the cell "No preferred server" in the column "Preferred server". A selection menu appears. Click on the OS server that you wish to designate as the preferred server for the OS client.
   The preferred servers available for selection are derived from the redundancy configuration of the OS server and passed to the OS client per package.
4. Close the dialog.
5. Repeat steps 1 and 3 for the second OS client. Make sure you set the redundant OS partner server as the preferred server for the second OS client.
6. Select the first OS and then select the menu command "Edit" > "Object Properties". In the dialog that opens activate the "Target OS and Standby OS" tab to set the path for the destination OS. Close the dialog window with the "OK" button. Follow the same procedure for the second OS.
7. All operator stations (OS servers and OS clients) are downloaded to the destination systems with the menu command "PLC" > "Download".
The "Configure Server Data" dialog on both OS clients may appear as follows:

- Dialog on OS client 1

- Dialog on OS client 2
3.5.9 How to Synchronize the Time on OS Clients to OS Servers

The WinCC "Time Synchronization" Editor is used to synchronize the time on OS clients to OS servers.

Note
The settings described below must be made on all the OS servers in use.

Requirements
- WinCC project must be opened on an OS client.
- OS clients communicate with the OS servers via the terminal bus.

Configuration
1. Open the WinCC "Time Synchronization" Editor.
2. If you activate the control box "Synchronization via the terminal bus (slave)", you have two options to synchronize the OS clients and OS servers via the terminal bus:

   By activating the option "Take time from integrated WinCC server", the time of day on the OS client is synchronized to an OS server from which the OS client has downloaded at least one package. This option does not provide any security against failure.

   When you activate the option "Take time from designated computer", you need to specify the computer name under "Computer 1". You can also specify a second computer under "Computer 2". In this case there is an automatic failover to Computer 2 if Computer 1 fails.

3. Close the dialog window with the "OK" button.
Further Topics

WinCC online help
3.5.10 How to Synchronize the Time on OS Servers to an External Time Generator

The WinCC “Time Synchronization” Editor is used to synchronize the time of day on OS servers to an external time generator, which is used as a master. The procedure described here relates to OS servers that are connected to a redundant system bus (Industrial Ethernet). Each of the two redundant OS servers has two 1613 communication processors. Furthermore, “Siclock TM” is used as the external time generator.

Note
The settings described below must be made on all the OS servers in use.

Requirements
- Two CP 1613 Industrial Ethernet communication processors installed and configured in an OS server.
- An external time source, e.g., Siclock TM, connected in the Industrial Ethernet.
- WinCC project must be opened on an OS server.

Configuration
1. Open the WinCC “Time Synchronization” Editor.
2. Activate the control box “Synchronization via system bus (master, slave)”.
3. For Device 1 select the CP where the time synchronization of the system bus should be performed. All installed CP’s are available for selection. Activate the “Master” option.
4. For Device 2 select the CP where the time synchronization of the system bus should be performed.
5. In the “Redundant Device” combination field select the CP for the connection to the system bus in case of failure of the first CP.
6. Close the dialog window with the “OK” button.
Once you have completed these steps, the "Time-of-day synchronization" dialog should appear as follows:

![Time Synchronization dialog]

Further Topics

- WinCC online help
- STEP 7 online help
- Operating Instructions GPS Converter GPSDEC/GPSCOM
- Operating Instructions SICLOCK Time Transmitter
3.6 SIMATIC BATCH

3.6.1 How to Configure a PC Station for a Redundant BATCH Server

A redundant BATCH server can be configured in SIMATIC PCS 7 to ensure that a batch process and the up-to-date batch data can continue to be controlled and monitored even when a BATCH server fails.

OS server with BATCH server

It is not possible to use a redundant PC as a common server for PCS 7 OS and SIMATIC BATCH.

Requirements

- Installed SIMATIC PCS 7 V6.0 software
- The following SIMATIC BATCH software packages for the redundant BATCH server:

<table>
<thead>
<tr>
<th>Software Package</th>
<th>BATCH Engineering</th>
<th>BATCH Server</th>
<th>BATCH Client</th>
<th>Single-user System (BATCH Single Station)</th>
</tr>
</thead>
<tbody>
<tr>
<td>BATCH Base</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>BATCH Builder</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>BATCH Client</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>BATCH Server</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>BATCH Fastobjects</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>BATCH WinCC Option</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BATCH Block</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

- A project created with SIMATIC PCS 7 V6.0 has to be open.
- The basic automation has to be configured, in other words, the AS hardware has to be configured and the CFC and SFC charts have to be created and compiled.

Configuration

1. If you have not already done so, set the view in the SIMATIC Manager to component view using the "View" menu.
2. Select your top project folder on the left side of the project window, open the context menu with a right mouse click and select "Insert new object". In the submenu, click on "SIMATIC PC Station".
3. Click the right mouse button on the inserted PC station and then select "Object Properties" in the context menu that opens. In the "Object Properties" dialog under the "General" tab enter the name of the computer where the PCS 7 project will be downloaded in the "Computer name" field.

Note:
You are responsible for entering the correct computer name. The system does not check if the computer name is correct.

4. Double-click on the inserted PC station in the left project window and then double-click on the "Configuration" components in the right project window to open HW Config.

5. In the "View" menu click on "Catalog". The hardware catalog opens. Select "Default" for the profile. Click on the plus sign in front of the "SIMATIC PC Station" folder to open its submenu. Click on the plus sign in front of "HMI" and then on "BATCH Application (stby)". Holding down the mouse button, drag the component to a free slot.

6. Save your current settings and close HW Config.

The configuration required for the SIMATIC PC station with a BATCH application (stby) should appear as follows in HW Config:

Further Topics
Manual and Online Help for SIMATIC BATCH
3.6.2 How to Configure a PC Station for a BATCH Client

BATCH clients use the batch data of a BATCH server in order to visualize it. The batch process is controlled and monitored on the BATCH client. The BATCH application client and WinCC application client are often run together on a SIMATIC PC station. The WinCC application client on the BATCH client enables the display of process messages. Both applications are configured in HW Config on a SIMATIC PC station.

Requirements

- Installed SIMATIC PCS 7 V6.0 software
- The following SIMATIC BATCH software packages for the BATCH client:

<table>
<thead>
<tr>
<th>Software Package</th>
<th>BATCH Engineering</th>
<th>BATCH Server</th>
<th>BATCH Client</th>
<th>Single-user System (BATCH Single Station)</th>
</tr>
</thead>
<tbody>
<tr>
<td>BATCH Base</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>BATCH Builder</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>BATCH Client</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>BATCH Server</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>BATCH Fastobjects</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>BATCH WinCC Option</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>BATCH Block</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

- A project created with SIMATIC PCS 7 V6.0 has to be open.
- The basic automation has to be configured, in other words, the AS hardware has to be configured and the CFC and SFC charts have to be created and compiled.

Configuration

1. If you have not already done so, set the view in the SIMATIC Manager to component view using the "View" menu.
2. Select your top project folder on the left side of the project window, open the context menu with a right mouse click and select "Insert new object". In the submenu, click on "SIMATIC PC Station".
3. Click the right mouse button on the inserted PC station and then select "Object Properties" in the context menu that opens. In the "Object Properties" dialog under the "General" tab enter the name of the computer where the PCS 7 project will be downloaded in the "Computer name" field.

Note:
You are responsible for entering the correct computer name. The system does not check if the computer name is correct.
4. Double-click on the inserted PC station in the left project window. In the right project window, double-click on the “Configuration” components to open HW Config.

5. In the “View” menu click on “Catalog”. The hardware catalog opens. Select “Default” for the profile. Click on the plus sign in front of the “SIMATIC PC Station” folder to open its submenu. Click on the plus sign in front of “HMI” and then on “Batch Application Client”. Holding down the mouse button, drag the component to a free slot.

6. Save your current settings and close HW Config.

The configuration required for the operator station with a BATCH application client should appear as follows in HW Config:

Further Topics

Manual and Online Help for SIMATIC BATCH
3.7 Component Replacement and System Modifications

3.7.1 Replacing Components During Online Operation

One crucial factor for uninterrupted operation of the fault-tolerant controller is the replacement of failed components during online operation. Replacement of defective components can only be accomplished when fault-tolerant automation components are used. When failure occurs, the automation system continues to operate due to its use of redundant components. The system is no longer fault-tolerant to the same level in such circumstances.

Failure and Replacement of Components in Central Racks and Expansion Racks

The following components in a redundantly configured AS can be replaced during operation:

- Central processing unit (e.g. CPU 417-4H)
- Power supply modules (e.g. PS 405, PS 407)
- Signal and function modules
- Communication modules
- Synchronization modules and fiber-optic cables
- Interface modules (e.g. IM 460, IM 461)

Note

Components in central racks cannot be replaced when powered.

Failure and Replacement of I/O Modules

The following components in a redundantly configured distributed I/O system can be replaced during operation:

- PROFIBUS-DP masters (CPU or CP in the AS)
- Redundant PROFIBUS-DP interface modules (e.g. IM 153-2 and 157)
- PROFIBUS-DP backups (e.g. ET 200M, ET 200iS)
- PROFIBUS-DP cables

Further Topics

Manual Automation System S7-400H; Fault-Tolerant Systems
3.7.2 Modification of the Standard Systems During Online Operation

A system modification occurs when a hardware component is added, removed or replaced by an identical component in a fault-tolerant system. A system modification is always associated with a software modification since the changed hardware first has to be configured in "HW Config" and then downloaded to CPU. Only then can the changed hardware be physically replaced, removed or added.

Similar to the events that occur when components are replaced, when the system is modified during online operation, the functions of the modified components are taken over by the corresponding redundant components. The operating program is therefore not interrupted.

Note
You should carefully read the procedure described for PCS 7 in the manual, Automation Systems S7-400H; Fault-tolerant Systems, Chapter 10, Modifications to the System During Operation. Violation of one or more rules may result in reduced availability of the fault-tolerant system or even failure of the entire process control system.

Requirements

- The hardware components involved have to tolerate removal and insertion under power.
- Fault-tolerant system with CPU 414-4H or 417-4H with firmware version V2.0.0 or later

Which components can be modified?

Changes in the CPU

- Changes to the CPU parameters
- Changes to the memory components of the CPU

Adding or removing modules in the central or expansion devices

- Signal and function modules
- Communication modules
- Interface modules (e.g. IM 460, IM 461), only without power
- Use of a free channel or reconfiguration of a used channel on an existing module
Adding or removing modules components in distributed I/O modules

- DP backups with redundant interfaces (e.g. ET 200M, DP/PA-Link, Y-Link)
- Non-redundant DP backups in any DP master system
- Modules in modular DP backups
- DP/PA coupler
- PA devices (process automation)
- Use of a free channel or reconfiguration of a used channel on an existing module

Further Topics

STEP 7 online help

Manual Automation System S7-400H; Fault-Tolerant Systems

Manual Modification of the System During Online Operation Using CiR
4  Failure, Failover and Restarting Fault-tolerant Components

4.1  I/O Modules

4.1.1  Redundant Interfaces

Redundant interface modules are installed as modules in the distributed I/O device ET 200M and used to form the interface to the AS through the PROFIBUS-DP. They are always double, that is, they operate in "Redundant" system mode. When one of the two modules fails, bumpless failover is performed in the automation process to enable the second interface module.

Failure

When the active IM 153-2 interface module fails, bumpless failover to the redundant interface occurs. The master identification changes from the failed interface module to the newly activated interface.

When the redundant interface module fails, the master identification does not change.

Restart

When the failed interface module restarts, the redundant interface module keeps the master identification. The master identification only changes back to the first or repaired module when another failover occurs due to failure of the redundant interface.
4.1.2 **Redundant I/O Modules**

When a fault occurs in one of the redundantly configured modules, bumpless failover is performed to the second module which then takes over the signal processing.

**Failure Scenarios**

The following faults may occur in a module:

- Hardware or power failure in the module
- Signal disruption detected (e.g., wire break)
- Fault in the assigned bus segment to an IM 153-2

The failure of a signal is detected by the driver block. The corresponding module is then disabled and only the signal of the redundant module is used. A "disabled" module is defined as a module from which the function blocks no longer access data.

**Discrepancy**

If a discrepancy is detected between the input signals, a configurable discrepancy time is started. If the discrepancy remains even after the discrepancy time, no module will be disabled. During a renewed signal change, the module in which a signal change does not occur is disabled. This discrepancy analysis is performed in the cyclic OB's during the processing of user data (OB1 or OB30 to OB38).

An entry is also made in the diagnostics buffer and a corresponding OS message is generated. The status of the redundant modules can be evaluated by the corresponding driver blocks.

**Depassivation**

Repaired or new modules can be exchanged during online operation and reintegrated with their redundant partners.

Disabled modules are reactivated by the following events:

- When fault-tolerant system starts up
- When the fault-tolerant system switches to the "Redundant" operating mode
- Following a plant modification in RUN mode (CiR)
- When OB83 (insert/remove interrupt) is called by removing and reinserting a module.

Depassivation is performed automatically when one of these events occur.

**Note**

If an automatic depassivation is not started, for example, after replacing a faulty encoder, the removal and reinsertion of any module will trigger an overall depassivation.
4.2 Automation Systems

4.2.1 Failure of the Master CPU

The starting scenario for failure of a master CPU is that the S7-400H is in "Redundant" system mode. In other words, both CPU's of the fault-tolerant system are operating the user program synchronously and, as an example, CPU0 is the master CPU and CPU1 is the backup CPU. Event-driven synchronization ensures that there will be bumpless failover from the master CPU to the reserve CPU any time a failure occurs.

Example: Failure of the Master CPU

If CPU0 fails, the following LEDs light up on CPU1:

- REDF=Redundancy loss
- IFM1F=Interface fault on interface module 1, this points to the first fiber-optic cable (synchronization line)
- IFM2F=Interface fault on interface module 2, this points to the second fiber-optic cable (synchronization line)

The fault-tolerant system goes into "Solo" system mode, in other words, there is bumpless continuation in the operation of the user program by CPU1. CPU1 is now the master CPU. The fault-tolerant system is no longer in "Redundant" system mode, but is operating in a non-redundant state.

Example: A Failed Master CPU Comes Back Online

When the failed CPU0 comes back online it is not the master CPU. The connection and synchronization of the returning CPU0 is always carried out by the master CPU. Both processes are necessary in order check and synchronize the data in the memory of the master CPU and in the backup CPU. CPU0 then goes into RUN mode. Now the system is once again in "Redundant" mode.
4.2.2 Failure of a Fiber-Optic Cable

The starting scenario has the S7-400H in the "Redundant" system mode. The CPU in Rack 0 is the master CPU and the CPU in Rack 1 is the backup CPU. The operating mode switches of both CPU's are set to RUN or RUN-P.

Example: Failure of a Fiber-Optic Cable

When a fiber-optic cable fails, the LEDs REDF and IFM1F or IFM2F light up on the two CPU's depending on the location of the fiber-optic cable failure. The fault-tolerant system goes into the "Solo" system mode and the user program continues to be processed by the master CPU used up to this point (CPU0).

Example: CPU in Rack 1 Comes Back Online

Once the defective fiber-optic cable has been replaced and connected to both CPU's, the backup CPU, the CPU in Rack 1, now in STOP mode needs to be restarted.

There are several choices you can make:

- If you have access to the automation system, you can turn the key switch on the failed CPU from its current position (STOP) to the most recently used operating position (RUN, RUN-P).
- If there is an MPI connection to the fault-tolerant system, you can start the Rack 1 CPU in STOP using the "Operating Mode" dialog. Open the PCS 7 project on an ES and select the CPU in the right window section. Then click the right mouse button to open the "PLC" context menu and select "Operating Mode" to open the dialog.
- If there is an Industrial Ethernet connection to the fault-tolerant system, you can start the Rack 1 CPU in STOP using the "Operating Mode" dialog. Open the PCS project on an ES and click on the "Online" command in the icon bar of the SIMATIC Manager. In the dialog that opens, select a CPU and then click the right mouse button to open the "PLC" context menu and select "Operating Mode" to open the dialog.

In the second and third situation the "Operating Mode" opens.
Select the CPU in Rack 1 and click on "(Warm start)". The CPU in Rack 1 performs the connection and synchronization and the system is once again in "Redundant" system mode.

When the CPU in Rack 1 comes back online, the "Operating Mode" dialog appears as follows:
4.3 OS Servers

4.3.1 Failure, Failover and Restarting of Redundant OS Servers

This chapter presents conditions that lead to a change in the master/standby identification of an OS server and examples of how the system reacts to failure.

Failure Scenarios

- The project is not activated on the redundant OS partner server.
- Fault in the network connection from the OS server to the redundant OS partner server
- Fault in the network connection to OS clients
- Disrupted process connection to the AS

Reaction of WinCC Redundancy to Possible Disruptions

WinCC Redundancy can react to disruptions, faults or error messages in the following ways:

- The event and the point in time are saved.
- The failed OS server’s archives of the process data (Tag Logging), the message data (Alarm Logging) and the user data (User Archives) are synchronized with the archive data of the active OS server when the failed server comes back online.
- The system tags "@RM_MASTER" and "@RM_MASTER_NAME" are changed according to the situation.
- The OS clients automatically switch to the preferred server or to the remaining available OS server with master identification. The @RM_SERVER_NAME tag on an OS client indicates the OS server to which this OS client is currently connected.
- Control messages are generated in the message list.
The failure scenarios listed above and the resulting reactions by WinCC Redundancy are described in the following.

**Startup of an OS Server Pair**

In general, an OS server pair consists of the OS server and its OS partner server. The two PCs are configured with WinCC Redundancy to be a redundant node.

When the OS server pair starts up, WinCC Redundancy first checks which of the two OS servers is to be assigned the master identification. This depends on which OS server starts up first. If one OS partner server is active already when the other comes online, the second OS server receives the standby identification. If no other OS server is active when an OS server starts up, it is assigned the master identification.

The internal WinCC tag @RM_MASTER is set to indicate the master OS server and this tag is reset if an OS server is a standby. The "@RM_MASTER_NAME" tag contains the name of the OS server, for example, "Server 1". You can display this tag, for example, in an I/O field of a Graphics Designer image. These tags can also be evaluated by other applications or by scripts. The "@RM_MASTER" tag can also be changed.
WinCC Project is Deactivated

An operational WinCC project is activated on both OS servers. When the WinCC project is deactivated on OS Server 1 (master identification), the following reactions are triggered in WinCC Redundancy:

- OS Server 2 (standby identification) saves the time (date and time of day) of failure of OS Server 1 (master identification).
- OS Server 2 reports the failure of OS Server 1 with a process control message to the process control list on an OS client.
- OS Server 2 now takes over the role of the master by setting the @RM_MASTER tag. The @RM_MASTER_NAME tag is changed accordingly.
- If the WinCC project is activated again on OS Server 1, OS Server 1 is set as the standby and the @RM_MASTER tag is reset. The @RM_MASTER_NAME tags are changed accordingly.

Gaps in the archive data occur on OS Server 1 during the time it is not active. When OS Server 1 returns, the following actions are taken to remedy this:

- OS Server 2 saves the date and the time of day, marking the return of OS Server 1.
- OS Server 2 reports the return of OS Server 1 with a process control message to the message list.
- The data gaps in the message, process data and user archives of OS Server 1 are filled by the data from the OS Server 2 memory when the options "Synchronization of Tag Logging after the partner server comes back online" and "Synchronization of Alarm Logging after the partner server comes back online" in the "Redundancy" dialog are activated.
- The @RM_MASTER tags remain unchanged in the two OS servers; in other words, OS Server 2 keeps the master identification, @RM_MASTER remains set and the @RM_MASTER tag for OS Server 1 is reset.

Disrupted Network Connection to the OS Partner Server

A disrupted network connection is only detected in the redundancy scheme when it involves a fault in the stub, connector or in the network card.
The terminal bus as a whole remains unaffected; thus communication between the AS and OS servers is unaffected.

Both OS servers are started and processing an activated WinCC project. If a disruption in the network connection to the OS partner server occurs in this situation, WinCC Redundancy reacts as follows:

- Both OS servers save the date and time of day of the failure.
- Both OS servers report the failure with a process control message to the message list.
- If the disrupted OS server is a master, this changes the master/standby identification.

During the connection failure no online synchronization for alarm logging, operation messages and user archives can be performed between the two OS servers. The following actions are taken when the connection is restored:

- Both OS servers save the date and time of day of the restored connection.
- Both OS servers report the return with a process control message to the message list.
- Data from the alarm logging, tag logging and the user archives accumulated during the connection failure are transmitted to the returning OS server.
- The @RM_MASTER and @RM_MASTER_NAME tags remain unchanged in both servers.

**Disrupted Network Connection between the OS Client to the OS Server**

An OS Server and the OS client connected to it are processing an activated WinCC project. A redundant OS partner server has been configured for the OS server in WinCC Redundancy. The OS server is defined as the preferred server for the OS client. A disrupted network connection to the OS server may result from a broken cable in the stub from the network to the OS client. The terminal bus as a whole remains unaffected. If a connection failure occurs between the OS client to the OS server, WinCC Redundancy has the following reactions:

- The OS client is automatically switched from the failed OS server to its redundant OS partner server because the preferred server specified for the OS client is not available.
- When the failed OS server is available once again to the OS client, the OS client automatically switches back to its preferred server.
Disrupted Network Connection to the AS

If a fault occurs on the system bus connection between the OS server and the AS, WinCC Redundancy reacts as follows:

- The disruption of the system bus connection in the system bus is reported to the OS partner server.
- The OS partner server receives the message that the OS server has failed.
- The OS partner server saves the date and the time of day of the OS server failure.
- An OS client is automatically switched from the failed OS server to its redundant OS partner server when the option "Multi-client switch in case of a process connection error" in the "Redundancy" dialog is activated.

If the option "Synchronization after process connection error" in the "Redundancy" dialog under the "General" tab is activated, when the process connection to the OS server is restored, the missing data in the OS server memory is updated using the following procedure:

- The OS partner server saves the date and the time of day marking the return of OS server.
- The data gaps in the archives of the failed OS server are updated by the data from the memory of the OS partner server. The process data of all automation systems are synchronized. Even the process data of automation systems that have not failed are synchronized.
- When the process connection is restored, a process control message is sent to the message list.

Further Topics

WinCC online help
4.4 BATCH Servers

4.4.1 Failure reactions of BATCH servers

BATCH applications and, if configured, WinCC applications are active on BATCH servers. A BATCH client visualizes the batch data of the BATCH server to which it is connected.

Failure of the Master BATCH Server

When the master BATCH server fails, due to an operating system failure (blue screen) or an application error, for example, the standby BATCH server detects that the master is no longer available through the redundancy mechanism and takes over the master identification. An automatic failover then occurs in which the BATCH clients switch from the master BATCH server to the standby BATCH server.

The running BATCH program automatically continues following the failover to the redundant BATCH server. A status comparison is made between the active BATCH server and the AS. The BATCH program has to be manually triggered to continue if communication errors have occurred.

In a cluster solution, the external hard disk and associated BATCH data switches to the new master BATCH server. This makes the latest BATCH data available to the new master BATCH servers.

In a replication solution, the databases on the master BATCH server and the standby BATCH server are continually synchronized. If failover occurs between the BATCH servers, the new active BATCH servers always has access to the latest BATCH data.

Data Reliability

During the short failover time between the failed BATCH servers and its redundant BATCH server, no automation process data can be visualized on a BATCH client. Operator control commands are also lost during this period.

Further Topics

Manual and Online Help for SIMATIC BATCH
4.5 OS Clients

4.5.1 Failover Reactions of OS Clients for Continuous Operations

When a network interruption to the configured OS server occurs, the process values on the OS clients are no longer updated and the process control fails. Other OS clients connected to the redundant OS partner server are not affected by this. The plant operator can therefore change to these OS client if needed.

When OS Server 1 fails, OS Client 1 switches to redundant OS Server 2. The package loaded on the OS client determines the redundant partner server for OS Server 1. OS Client 1 is not available during the failover to OS Server 2. If the redundant OS Server 2 is specified as the preferred server for OS Client 2, however, the plant can continue to be controlled during the failover from the failed OS Server 1 to redundant OS Server 2.

When OS Server 1 becomes available again OS Client 1 switches back to the returned OS Server 1 because it is the configured preferred server. Continuous operation is restored once OS Client 1 has switched back. OS Client 1 is not available during the failover to OS Server 1. OS Client 2 remains operable.

The status of the "@RM_Master" redundancy tag does not apply to the OS client with preferred server configuration. The @RM_SERVER_NAME tag indicates the OS server to which this OS client is currently connected.
Reaction of an OS Client without a Preferred Server

If no preferred server is set on the OS client in the “Configure Server Data” dialog, the OS client connects to the redundant OS server on which the "@RM_Master" redundancy tag is set.

When the active OS server fails, its redundant OS partner server becomes the master server. The status of "@RM_Master" redundancy tag indicates which of the two redundant OS servers is currently acting as the master server. Setting or resetting this tag therefore triggers a manual switch in which all OS clients connect to the "new" master server.

OS Client Failover Scenarios

The following scenarios may trigger failover of the OS clients. It is not relevant here whether or not a preferred server is set.

- Disrupted network connection to the redundant OS server.
- Redundant OS server fails, e.g., due to power loss.
- WinCC project of the redundant OS server is deactivated.
- Disrupted network connection between OS server and AS, when the option “OS client switch in case of a process connection error” in the “Redundancy” dialog is activated.

Further Topics

WinCC online help
4.6 BATCH Clients

4.6.1 Failover Reactions of BATCH Clients

When the master BATCH server fails, the BATCH clients automatically switch to the redundant BATCH server.

Reactions during Failover

During failover a message window is displayed on the screen of the BATCH client indicating the failover. The BATCH client cannot be operated during this time. The message window disappears and the BATCH client can be operated once the failover from the failed BATCH server to the redundant BATCH server is completed.

Further Topics

Manual and Online Help for SIMATIC BATCH
5 Diagnostics

5.1 Diagnostics for Redundant Components and Systems

This chapter describes the testing and diagnostics features in PCS 7. You can use these features to analyze individual redundant components. PCS 7 offers the following diagnostic features:

**Diagnostics Using Software Programs**

<table>
<thead>
<tr>
<th>Program/Application</th>
<th>Component/Diagnostic Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Diagnostics</td>
<td>Reads the diagnostics buffer, CPU, modules capable of diagnostics, communication properties</td>
</tr>
<tr>
<td></td>
<td>e.g., CP’s, displays incoming process control messages in plain text</td>
</tr>
<tr>
<td>WinCC Diagnostics</td>
<td>Status of logical connections, tag status, WinCC channel diagnostics</td>
</tr>
<tr>
<td>Lifebeat Monitoring</td>
<td>Monitors all OS servers, OS clients and all automation systems</td>
</tr>
<tr>
<td>WinCC Scope</td>
<td>Diagnostics for WinCC projects</td>
</tr>
<tr>
<td>NetCC</td>
<td>NetCC enables you to manage and visualize network stations on which WinCC is installed.</td>
</tr>
<tr>
<td>Evaluation of WinCC</td>
<td>The following system tags can be evaluated in runtime, e.g., in an I/O field of a system image</td>
</tr>
<tr>
<td>Redundancy System Tags</td>
<td>in the Graphics Designer:</td>
</tr>
<tr>
<td></td>
<td>@RM_MASTER</td>
</tr>
<tr>
<td></td>
<td>@RM_MASTER_NAME</td>
</tr>
<tr>
<td></td>
<td>@RM_SWITCHER</td>
</tr>
<tr>
<td></td>
<td>@RM_UA_ONL_“Archive Name”</td>
</tr>
<tr>
<td></td>
<td>@RM_OFFLINE_UA_NAME</td>
</tr>
</tbody>
</table>

**Diagnostics Using LEDs**

LED displays provide local information about the status of a variety of redundant components.

<table>
<thead>
<tr>
<th>Redundant Hardware</th>
<th>Diagnostic Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>PS (power supply)</td>
<td>LEDs</td>
</tr>
<tr>
<td>CPU (central processing unit)</td>
<td>LEDs</td>
</tr>
<tr>
<td>CP (communication processor)</td>
<td>LEDs</td>
</tr>
<tr>
<td>IM (interface module)</td>
<td>LEDs</td>
</tr>
<tr>
<td>SM (signal module - digital/analog I/O</td>
<td>LEDs</td>
</tr>
<tr>
<td>module)</td>
<td></td>
</tr>
</tbody>
</table>

**Further Topics**

Manual Service Support and Diagnostics
5.2 Reporting, Testing and Monitoring

5.2.1 Hardware Diagnostics

Hardware diagnostics provide dynamic information about the operating mode of modules, even for CP's in S7 station connected online. You can interpret diagnostics information for a module from the diagnostics icons in the project window of the SIMATIC Manager.

Diagnostics icons show the status of the corresponding module and the operating mode of CPU's.

Detailed diagnostics information is displayed in the "Module Information" window, which you can call up by double-clicking on a diagnostics icon in quick view or diagnostics view.

Communication Diagnostics with NCM S7 Diagnostics

NCM S7 diagnostics provides dynamic information about the operating mode of communication functions of CP's connected online.

HW Config Provides Static Information

HW Config provides static information about the hardware configuration. This means you have continuous information about the configured communication properties of CP's connected online or offline.

Further Topics

- STEP 7 online help
- Manual SIMATIC NET NCM S7 for Industrial Ethernet
- Manual SIMATIC NET NCM S7 for PROFIBUS
- Manual SIMATIC NET S7 CP's for Industrial Ethernet
5.2.2 WinCC Diagnostics

WinCC offers the following diagnostic features for the communication connection between a WinCC project and a SIMATIC S7 station:

- Diagnostics for the communication connection in the WinCC Explorer on an OS server. The WinCC project needs to be active for this. A dialog for monitoring all of the configured connections can be opened in the WinCC Explorer with the menu command "Options" > "Status Connections". All configured connections are listed in the "Status Logical Connections" window. The displayed values represent the current status and are updated cyclically.

- WinCC tag management offers another method of obtaining information about the connection status in general and individual tags in particular. The status of a configured connection can be obtained by positioning the mouse pointer on a connection. Brief information then appears showing "Status: OK" or Status: "Disconnected". The current process value of a specific tag, as well as its status, can also be obtained by positioning the mouse pointer.

- Diagnostics for the communication connection using the WinCC Channel Diagnostics program. The program is started with the command "Start" > "Simatic" > "WinCC" > Tools "Channel Diagnostics". Detailed information about the status of each configured connection is displayed in the "Channels/Connections" tab. The display is updated every second by default. The update cycle can be set in the lower entry field. When a connection is disrupted, the cause of the disruption is indicated by a specific value in the "Error Code" line in the right window.
Further Topics

WinCC online help
5.2.3 **Lifebeat Monitoring**

Lifebeat Monitoring is a program that is used for monitoring all OS server PCs, all OS client PCs and all automation systems in an active WinCC project. To accomplish this, all network nodes have to be available through PC networks and industry networks.

All connected nodes available through the networks are displayed in a system image in WinCC.
The communication between WinCC and the automation systems is established through a channel. The configuration of the lifebeat monitoring is made through an OPC connection.
In a distributed redundant system, the following points should be taken into consideration when configuring lifebeat monitoring:

- Lifebeat monitoring of an OS server pair monitors its lower-level automation systems and all other OS servers.
- Monitoring of the OS clients should be distributed to several OS server pairs.
- Configure only those OPC connections to OS clients that are actually being monitored. When an OS client is removed from the network, the corresponding OPC connection should be deleted.

Further Topics
WinCC online help

5.2.4 WinCC Scope

WinCC Scope offers diagnostics for WinCC projects. It provides a wide range of information about the active project as well as the computer system being used.

Requirements
- Internet Explorer or Netscape Navigator
- TCP/IP network protocol
- Installation of WinCC, including an installed version of Scope
- The "WinCCDiagAgent.exe" program has to be started. It is located in the directory, Siemens\WinCC\WinCCScope\bin.

WinCC Scope can then be started with the following command in the start menu.
Start > Simatic > WinCC > Tools > Scope

The link on the starting page, “How to Use the New Diagnostics Interface”, provides a general description about the operation of WinCC Scope. Click on the link http://localhost to start Scope. A variety of information can be called up from the list in the left window. The System Info section offers general information about the current computer system. The WinCC Info section provides information about the currently active WinCC project.
Further Topics

WinCC online help
5.2.5 NetCC

NetCC enables you to manage and visualize network stations on which WinCC is installed.

NetCC offers:

- Graphic visualization of the stations in an overview display
- Information about each station (password protected if needed)
- Commands on remote station (password protected if needed)

This enables centralized administration of all WinCC systems integrated in the network.

How NetCC Works

NetCC consists of the following components:

- Display in WinCC Explorer

  A list of networked WinCC stations is displayed in the WinCC Explorer.

  The configuration dialog for NetCC can be called up here. You can also request information for every individual station and issue commands on the network station from the list of network stations.

- CC Agent

  CC Agent manages the communication and the data exchange between the networked WinCC stations in the background.

- NetCC Viewer

  NetCC Viewer is used to visualize networked WinCC stations.

  You can call up information about each individual station or issue commands on the network station from the display.

- NetCC Viewer uses ActiveX controls

  In the Graphics Designer, you can insert the NetCC Viewer in a process image as a "NetCC Viewer Control" ActiveX control.

  The following features are available:

  You can configure the NetCC Viewer controls in the Graphics Designer.

  The complete functionality of the stand-alone NetCC Viewer is available in runtime.
Licensing

A separate license is required for NetCC. The authorization must be installed on each NetCC station.

Without authorization a station may be viewed by other network stations, but no information can be obtained and no commands can be executed. NetCC utilities, such as the NetCC Viewer, also cannot be used on non-licensed stations.

Further Topics

WinCC online help
6 Parameters of Fault-tolerant Process Control Systems

6.1 Parameters of Fault-tolerant Process Control Systems

Overview

This chapter provides a brief introduction to the parameters of fault-tolerant process control systems and describes the practical effects of redundant design using a few selected configurations.

The reliability and availability parameters are usually needed for quantitative assessment of fault-tolerant process control systems. These parameters are defined below.

Reliability

Reliability is the characteristic of a technical device to fulfill its function during its operating period. This is usually no longer possible when a component fails. The criterion frequently specified for reliability is therefore MTBF (Mean Time Between Failure). It can be determined statistically for systems in operation or by calculating the failure rates of the components used in the design of the module.

Reliability of Modules

The reliability of SIMATIC components is extremely high due to the extensive quality assurance measures applied in development and manufacture. The following average values apply to SIMATIC modules, which are calculated more conservative than the industry at large:

- MTBF of a central processing unit: 15 years
- MTBF of an I/O module: 50 years
Reliability of Automation Systems

The use of redundant modules greatly increases the MTBF of a system. Almost all errors can be detected and localized using the high-performance self-tests and the mechanisms for error detection that are integrated in the CPU's of the S7-400H. The diagnostic coverage (dc) is approximately 95%. Starting from the reliability of a single system (1-out-of-1 systems having an MTBF 1001), it is possible to calculate the reliability of the S7-400H as a dual-channel (2-out-of-2) fault-tolerant system using the following formula:

\[
MTBF_{1v2} = \frac{[MTBF_{1v1}]^2}{2MDT + [2(1-dc)MTBF_{1v1}]}
\]

The MTBF of the S7-400H is determined by its MDT (Mean Down Time). This time essentially consists of the time for error detection and for repair or replacement of defective modules. The error detection time is half the configured test cycle time (by default, 90 min.). The repair time for a modular system such as the S7-400H is normally four hours.

Availability

Availability is the probability of a system being capable of operation at a specified point of time. It can be enhanced by redundancy, such as the use of redundant I/O modules or the use of multiple sensors at a measuring point. Redundant components are configured in such a way that system operability is not affected by the failure of a single component. Here, again, a detailed diagnostic display is an essential factor for availability. The availability of a system is expressed as a percentage. It is determined by the mean time between failure (MTBF) and the mean time to repair (MTTR). The availability of a dual-channel (2-out-of-2) fault-tolerant system can be calculated using the following formula:

\[
V = \frac{MTBF_{1v2}}{MTBF_{1v2} + MDT} \times 100\%
\]

Further Topics

Manual Automation System S7-400H; Fault-Tolerant Systems
Glossary

The following are a few important terms which may be needed or helpful in understanding this documentation and related material.

One-out-of-two system

A fault-tolerant system in which the system components are doubled. When one component fails, the second, redundant components takes over the entire system (failover). One of the two components is therefore always in operation.

10BASE-T

Standard for 10 Mbaud Ethernet transmission on Twisted Pair cables

100BASE-T

Fast Ethernet Standard (100 Mbaud) for data transmission on Twisted Pair cables

Active redundancy

All redundant resources are constantly in operation and are simultaneously involved in the execution of the control task.

The S7-400 consists of two redundantly configured subsystems, which are synchronized through fiber-optic cables. The two subsystems form a fault-tolerant automation system that operates with a dual-channel design (1-out-of-2) according to the principle of "active redundancy".

Active redundancy, often referred to as functional redundancy, means that all redundant components are in continual operation and are simultaneously participating in the processing control tasks. For the S7-400H, this means that the user program loaded in both CPU's is fully identical and is run synchronously by both CPU's.

Link-up

In the link-up system mode of a fault-tolerant system the master CPU and the standby CPU compare the memory configuration and the contents of the load memory. If they establish differences in the user program, the master CPU updates the user program of the standby CPU.
Automation System

An automation system consists of a variety of hardware components and integrated system functions depending on the system it is designed to control. In PCS 7, this involves the following components:

- Mounting rack with 9 or 18 slots, some are separated for redundant systems
- CPU's 414-3, 416-2, 416-3 or 417-4 and redundant CPU's 414-4H and 417-4H
- Power supply DC 24 V or AC 120/230 V
- RAM 768 to 20 MB
- Memory card with 1 to 8 MB
- Runtime license for libraries, driver blocks / technological blocks
- Connection to Industrial Ethernet, e.g. CP 443-1
- Connection to PROFIBUS as the DP master or for S7 communication

Update

In the update system mode of a fault-tolerant system, the master CPU updates the dynamic data of the standby CPU (synchronization).

AS

See automation system

Backbone

Highest level of a hierarchically structured network system.

BCE

Basic Communication Ethernet. A simple Ethernet communication solution.

Bus

A common transfer route connecting all notes and having two defined ends. For Industrial Ethernet the bus takes the form of a segment with triaxial cable and a bus coupler.

Cold standby

Local warehousing of replacement parts. Simple replacement of a subsystem and a cold restart of the master when a failure occurs.

CPU

The central processing unit of the S7 automation system containing the control, arithmetic and logic units, memory, operating system and interface for the programming device.
Diagnostics

Diagnostics involves the detection, localization, classification, display and advanced analysis of errors, faults and messages. Diagnostics includes monitoring functions that are executed automatically while the system is operating. This increases the availability of system by reducing the installation time and downtime.

Diagnostic interrupt

Diagnostics-compatible modules use diagnostic interrupts to notify the central CPU of system errors. In SIMATIC S7: When an error is detected or ceases (e.g. wire break), the module triggers a diagnostic interrupt, provided the interrupt is enabled. The CPU interrupts the processing of the user program and lower priority classes and processes the diagnostic interrupt block (OB 82).

Diagnostics buffer

The diagnostics buffer is a buffered memory area for CPU's in which diagnostic events are saved in the sequence they occur.

DP address

Each bus node is assigned a unique DP address on the PROFIBUS-DP for its identification. A PC, programming devices or ET 200 handhelds have the DP address "0". DP masters and DP backups have a DP address in the range of 0 to 125.

Error handling via OB

When the operating system detects a specific error (e.g. access error in STEP 7), it calls a dedicated organization block (Error OB) that determines the subsequent response of the CPU.

Error display

The error display is one of the possible responses of the operating system to a runtime error. The other possible responses are:

Error response in the user program and STOP mode for the CPU or IM 153-1.

Fail-safe system

A system that can be brought to a safe stop in order to protect life, the environment and capital.

Field level

An automation system as a whole consists of the management (HMI), process and field I/O levels. Field devices are used on the field-I/O level. Motors, valves, actuators and sensors are examples of field devices.
Full duplex
The ability of a device to send and receive data simultaneously. Collision detection is deactivated for full-duplex operation.

Half duplex
A device can either send or receive data at a given time but not both.

HART
Abbreviation for "Highway Addressable Remote Transducer". HART devices are actuator and sensors that can be configured per HART protocol.

Fault-tolerant system
A system that automatically switches to a standby system when failure occurs (failover). Both hardware and software components are used for this purpose. The standby system is also referred to as the redundant system.

Hot standby
Fully bumpless failover to a standby system. This requires parallel control processing by the standby system in order for it to be capable of continuing the ongoing control processing when the master system fails.

During normal operation, the master handles the process communication and the other functions are handled by both systems (functional redundancy complying to DIN 40041). There are hardware and software based solutions for parallel processing. Hot standby is required when, in case of failure by the master, the standby system needs past values that are no longer available from the process and bumpless failover is an absolute necessity. Fast transfer of all the process data from the master system to the standby system is not a solution since this involves the danger of corrupt data being passed along to the standby system, thereby threatening bumpless failover. Full redundancy can only be guaranteed by parallel, redundant processing of the signals in both subsystems.

Fault-tolerant station
A station containing two central processing units (master and standby).

H System
Fault-tolerant system consisting of at least two central processing units (master and standby). The user program is processed identically in both the master and standby CPU’s.

Hub
Active network components with repeater functionality, synonym for star coupler.
ITP
Industrial Twisted Pair: bus system for industrial application based on the Twisted Pair standards IEEE 802.3i: 10BASE-T and IEEE 802.3j: 100BASE-TX.

Management level (HMI)
An automation system as a whole consists of the management (HMI), process and field I/O levels. The management level (HMI) is formed by PCs which are used as clients, multi-clients and servers to control and monitor the process.

Control system
An assembly of components which can be used to monitor, control and regulate industrial production processes.

Fiber-optic cable (FO)
Fiber-optic cable is a transmission medium in an optical network. Only multimode glass fiber-optic cables are suitable for connecting optical Industrial Ethernet components.

Master CPU
The central processing unit that is the first redundant central processing unit to start up. It continues to operate as the master when the redundancy connection is lost. The user program is processed identically in both the master and standby CPU's.

Media redundancy
Redundancy in the network infrastructure (cables and active components such as OLM's or OSM/ORM's).

OLM
Optical Link Module. Industrial Ethernet network component with repeater functionality.

OSM
Optical Switch Module. Industrial Ethernet network component with switch functionality. Offers the features of a redundancy manager. Controls the media redundancy in an OSM ring.
Passive standby (redundancy):

Only one system is active in normal operation. The second system is on standby and takes over the function of the first system if it fails.

The disadvantage of such a system is that the standby system does not have access to the current process data. If failure occurs, this increases the failover time because the standby system can only continue the process once it has loaded this data.

The operability of the standby system is not permanently checked, if the first system fails and the standby system also fails and cannot take over the processing.

Process level

An automation system as a whole consists of the management (HMI), process and field I/O levels. The process level is formed by the automation systems and interface modules.

Redundancy

The existence of more than one resource in a device to execute a required function. In the context of automatic regulation and control, these resources are usually devices or software programs.

In PCS 7 redundancy means that one subsystem (master system) controls the process and the other subsystem (standby system) is in reserve and ready to take over in case of failure. Standby does not mean, however, that this subsystem has no function.

Standby CPU

The redundant central processing unit of a fault-tolerant system that is linked to the master CPU. It goes to STOP mode when the redundancy connection is lost. The user program is processed identically in both the master and standby CPU's.

Signal module (I/O modules)

Signal modules form the interface between the process and the automation system. Input/output modules can be digital or analog.

System diagnostics

System diagnostics involve the detection, analysis and reporting of faults that occur in the automation system. Program errors or module failures are examples of such faults. System faults can be displayed with LEDs or in STEP 7.

Solo mode

In the solo system mode of a fault-tolerant system, the master CPU is in RUN mode, whereas the standby CPU is in the STOP, ERROR-SEARCH or DEFECTIVE mode.
Availability

Availability is traditionally defined as the quotient MTBF / (MTBF + MTTR) - or in short form: actual operating condition / nominal operating condition. Based on this definition, the basic availability of a standard component or a standard system can be increased by increasing the MTBF ("better quality" or reliability) and/or by decreasing the period necessary for repairs (MTTR).

MTBF - mean time between failure
MTTR - mean time to repair

Warm standby

Fast continuation of an interrupted function at a reinsertion point.
# Index

## A
- actuators ............................................... 2-12
- AS ......................................................... 2-13
  - components ........................................ 2-13
  - method of operation ................................ 2-16
- assigning S7 programs ................................ 3-33
- automation system ..................................... 2-13
  - hardware components ................................ 2-13
  - how the S7-400H operates .......................... 2-16

## B
- BATCH clients ............................................ 2-14
  - failover reactions .................................. 4-14
- BATCH flexible ........................................ 2-35
- batch process .......................................... 2-35
- BATCH servers ......................................... 2-37
- bumpless transfer ....................................... 1-4

## C
- central processing unit ................................ 2-13
- changes to the CPU ..................................... 3-50
- client .................................................... 2-38
- cluster ................................................... 2-35
- communication connections ......................... 2-35
  - configuring ......................................... 3-10
  - communication lines ................................ 2-17
  - communication module ................................ 2-13
  - communication solutions ......................... 2-17
  - redundant field bus ................................. 2-20
  - redundant system bus ............................... 2-22
  - redundant terminal bus .............................. 2-26
- compiling/downloading programs/.................. 3-36
- component replacement ................................ 3-49
- components of S7-400H ................................ 2-13
- configuration .......................................... 3-36
- configuration notes .................................... 3-1
- configuring a BATCH client ......................... 3-47
- configuring a bus interface ......................... 3-16
- configuring a client ................................... 3-37
- configuring a field bus ................................ 3-10
- configuring a redundant BATCH server ............ 3-45
- configuring a terminal bus ............................ 3-15
- configuring an OS ....................................... 3-28
- configuring the DP/PA-Link ......................... 3-24
- configuring WinCC Redundancy ....................... 3-34
- configuring Y-Link ..................................... 3-21
- continuous operation ................................. 2-38
- CP ......................................................... 3-5

## D
- definition of fault tolerance ......................... 1-13
- downloading to PLCs ................................ 3-36
- DP/PA coupler .......................................... 3-24
  - 3-25
- DP/PA-Link ............................................. 2-9

## E
- electrical ring ........................................ 2-17
- engineering station .................................... 2-39
  - 2-40
- ES ......................................................... 2-39
  - 2-40
- ESM ....................................................... 2-19
- ET 200M .................................................. 2-6
  - configuring a bus interface ....................... 3-16
  - expansion components for ET 200 M ............ 3-16
  - external time generator ............................ 3-43

## F
- failure and replacement of components ............. 3-49
- Failure reactions ....................................... 4-11
  - BATCH server ........................................ 4-11
  - fiber-optic cable .................................... 4-4
  - Master CPU .......................................... 4-3
  - redundant I/O modules ............................. 4-2
  - redundant interface ................................ 4-1
  - redundant OS server ................................ 4-6
  - fault tolerance ....................................... 1-13
  - fault-tolerant automation system ................ 2-13
  - fault-tolerant process control system .......... 1-2
  - fault-tolerant process control systems
    - parameters ........................................ 6-1
  - features for servicing .............................. 1-13
  - features for the operation phase ................ 1-11
  - fiber-optic cables .................................. 2-14
  - 2-15
  - field bus ............................................ 2-20
  - configuration and components ........................ 2-20
  - for the configuration phase ....................... 1-10

## H
- H station .................................................. 3-2
### Index

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>How to import GSD files</td>
<td>3-27</td>
</tr>
<tr>
<td>I</td>
<td></td>
</tr>
<tr>
<td>I/O</td>
<td>2-1, 2-2, 2-3, 2-4</td>
</tr>
<tr>
<td>configuration rules</td>
<td>2-6</td>
</tr>
<tr>
<td>design rules</td>
<td>2-6</td>
</tr>
<tr>
<td>distributed</td>
<td>2-1, 2-2</td>
</tr>
<tr>
<td>DP/PA-Link</td>
<td>2-9</td>
</tr>
<tr>
<td>expansion components for ET 200M</td>
<td>2-7</td>
</tr>
<tr>
<td>I/O device ET 200M</td>
<td>2-6</td>
</tr>
<tr>
<td>PROFIBUS connection</td>
<td>2-12</td>
</tr>
<tr>
<td>redundant</td>
<td>2-4</td>
</tr>
<tr>
<td>redundant actuators and sensors</td>
<td>2-12</td>
</tr>
<tr>
<td>redundant I/O modules</td>
<td>2-7</td>
</tr>
<tr>
<td>redundant interface module</td>
<td>2-7</td>
</tr>
<tr>
<td>single-channel switched distributed I/O</td>
<td>2-3</td>
</tr>
<tr>
<td>Y-Link</td>
<td>2-11</td>
</tr>
<tr>
<td>I/O device ET200M</td>
<td>2-6</td>
</tr>
<tr>
<td>I/O modules</td>
<td>3-18</td>
</tr>
<tr>
<td>IM 153-2</td>
<td>2-7, 3-16</td>
</tr>
<tr>
<td>inserting a SIMATIC H station</td>
<td>3-2</td>
</tr>
<tr>
<td>inserting and removing modules</td>
<td>3-50</td>
</tr>
<tr>
<td>inserting communication processors</td>
<td>3-5</td>
</tr>
<tr>
<td>inserting synchronization modules</td>
<td>3-3</td>
</tr>
<tr>
<td>interface module IM153-2</td>
<td>2-7</td>
</tr>
<tr>
<td>M</td>
<td></td>
</tr>
<tr>
<td>mounting racks</td>
<td>2-14</td>
</tr>
<tr>
<td>multi-project engineering</td>
<td>2-41</td>
</tr>
<tr>
<td>N</td>
<td></td>
</tr>
<tr>
<td>NetCC</td>
<td>5-9, 5-10</td>
</tr>
<tr>
<td>notes about configuration</td>
<td>3-1</td>
</tr>
<tr>
<td>O</td>
<td></td>
</tr>
<tr>
<td>optical PROFIBUS</td>
<td>2-20</td>
</tr>
<tr>
<td>optical ring</td>
<td>2-18</td>
</tr>
<tr>
<td>OS client</td>
<td>2-38</td>
</tr>
<tr>
<td>additional</td>
<td>2-38</td>
</tr>
<tr>
<td>configuring</td>
<td>3-37</td>
</tr>
<tr>
<td>HMI continuous operation</td>
<td>2-38</td>
</tr>
<tr>
<td>OS Clients</td>
<td></td>
</tr>
<tr>
<td>failover reactions</td>
<td>4-12</td>
</tr>
<tr>
<td>OS server</td>
<td>2-29, 2-32, 2-33, 2-34</td>
</tr>
<tr>
<td>failure</td>
<td></td>
</tr>
<tr>
<td>failover and restarting</td>
<td>4-6</td>
</tr>
<tr>
<td>method of operation</td>
<td>2-29</td>
</tr>
<tr>
<td>time synchronization</td>
<td>2-31</td>
</tr>
<tr>
<td>OS terminal</td>
<td>2-38</td>
</tr>
<tr>
<td>OSM</td>
<td>2-17</td>
</tr>
<tr>
<td>overview of components</td>
<td>1-1</td>
</tr>
<tr>
<td>P</td>
<td></td>
</tr>
<tr>
<td>parameters of fault-tolerant process control systems</td>
<td>6-1</td>
</tr>
<tr>
<td>PC station</td>
<td>2-40</td>
</tr>
<tr>
<td>PCS 7 overview of features</td>
<td>1-9</td>
</tr>
<tr>
<td>features for servicing</td>
<td>1-13</td>
</tr>
<tr>
<td>features for the configuration phase</td>
<td>1-10</td>
</tr>
<tr>
<td>features for the operation phase</td>
<td>1-11</td>
</tr>
<tr>
<td>PCS 7 process control system</td>
<td>1-1</td>
</tr>
<tr>
<td>PLC</td>
<td>3-36</td>
</tr>
<tr>
<td>power supply</td>
<td>2-14</td>
</tr>
<tr>
<td>preferred server</td>
<td>2-39</td>
</tr>
<tr>
<td>PROFIBUS connection</td>
<td>2-12</td>
</tr>
<tr>
<td>R</td>
<td></td>
</tr>
<tr>
<td>redundancy concept</td>
<td>1-5</td>
</tr>
<tr>
<td>Redundancy Nodes</td>
<td>1-14</td>
</tr>
<tr>
<td>redundant BATCH server</td>
<td>2-35</td>
</tr>
<tr>
<td>redundant communication</td>
<td></td>
</tr>
<tr>
<td>connections</td>
<td>3-10</td>
</tr>
<tr>
<td>configuring a field bus</td>
<td>3-10</td>
</tr>
<tr>
<td>configuring a terminal bus</td>
<td>3-15</td>
</tr>
<tr>
<td>configuring the system bus</td>
<td>3-13</td>
</tr>
<tr>
<td>redundant communication processors</td>
<td>3-5</td>
</tr>
<tr>
<td>redundant connection between OS and AS</td>
<td></td>
</tr>
<tr>
<td>redundant I/O</td>
<td>3-31</td>
</tr>
<tr>
<td>redundant OS server</td>
<td>2-4</td>
</tr>
<tr>
<td>configuring</td>
<td>3-28</td>
</tr>
<tr>
<td>redundant OS servers</td>
<td>2-29, 2-30</td>
</tr>
<tr>
<td>redundant system bus</td>
<td>2-22, 2-23</td>
</tr>
<tr>
<td>repair time</td>
<td>1-4</td>
</tr>
<tr>
<td>replication</td>
<td>2-35, 2-36</td>
</tr>
<tr>
<td>S</td>
<td></td>
</tr>
<tr>
<td>S7-400H</td>
<td>2-16</td>
</tr>
<tr>
<td>hardware components</td>
<td>2-13</td>
</tr>
<tr>
<td>Scope</td>
<td>5-7</td>
</tr>
<tr>
<td>sensors</td>
<td>2-12</td>
</tr>
<tr>
<td>server</td>
<td>2-29, 2-30, 2-31</td>
</tr>
<tr>
<td>setting the project paths</td>
<td>3-30</td>
</tr>
<tr>
<td>signal modules</td>
<td>3-18</td>
</tr>
<tr>
<td>SIMATIC PC station</td>
<td>3-36, 3-37</td>
</tr>
<tr>
<td>compiling an OS</td>
<td>3-33</td>
</tr>
<tr>
<td>configuring a BATCH client</td>
<td>3-47</td>
</tr>
<tr>
<td>configuring a redundant BATCH server</td>
<td></td>
</tr>
<tr>
<td>configuring WinCC Redundancy</td>
<td>3-45</td>
</tr>
<tr>
<td>redundant connection between AS and OS</td>
<td>3-31</td>
</tr>
<tr>
<td>setting the project paths</td>
<td>3-30</td>
</tr>
<tr>
<td>Index</td>
<td>Page</td>
</tr>
<tr>
<td>-------</td>
<td>------</td>
</tr>
<tr>
<td>PCS 7 Fault-tolerant Process Control System</td>
<td>1-5</td>
</tr>
<tr>
<td>SIMATIC PCS 7 overview of features</td>
<td>1-9</td>
</tr>
<tr>
<td>for servicing and system expansion</td>
<td>1-13</td>
</tr>
<tr>
<td>for the configuration phase</td>
<td>1-10</td>
</tr>
<tr>
<td>for the operation phase</td>
<td>1-11</td>
</tr>
<tr>
<td>SIMATIC PCS 7 redundancy concept</td>
<td>1-5</td>
</tr>
<tr>
<td>single-channel switched</td>
<td>2-1</td>
</tr>
<tr>
<td>solutions for I/O</td>
<td>2-3, 2-6</td>
</tr>
<tr>
<td>sync module</td>
<td>3-3</td>
</tr>
<tr>
<td>inserting</td>
<td>3-3</td>
</tr>
<tr>
<td>synchronization</td>
<td>3-41, 3-43</td>
</tr>
<tr>
<td>synchronization module</td>
<td>2-14</td>
</tr>
<tr>
<td>system modifications during online operation</td>
<td>3-50</td>
</tr>
<tr>
<td>T</td>
<td>3-41, 3-43</td>
</tr>
<tr>
<td>time generator</td>
<td>2-31, 3-41, 3-43</td>
</tr>
<tr>
<td>time synchronization</td>
<td>3-8</td>
</tr>
<tr>
<td>W</td>
<td>2-38</td>
</tr>
<tr>
<td>WinCC client</td>
<td>2-38</td>
</tr>
<tr>
<td>WinCC server</td>
<td>2-29</td>
</tr>
<tr>
<td>Y</td>
<td>2-11</td>
</tr>
<tr>
<td>Y-Link</td>
<td>2-11</td>
</tr>
</tbody>
</table>