SIEMENS

SIMATIC

Fault-tolerant Systems S7-400H

System Manual

Preface 1

Fault-tolerant automation systems 2

S7-400H installation options 3

Getting started 4

Installation of a CPU 41x–H 5

Special functions of a CPU 41x-H 6

S7–400H in PROFIBUS DP mode 7

System and operating states of the S7–400H 8

Link-up and update 9

Using I/Os in S7–400H 10

Communication 11

Configuring with STEP 7 12

Failure and replacement of components during operation 13

System modifications in operation 14

Synchronization modules 15

S7-400 cycle and reaction times 16

Technical data 17

Characteristic values of redundant automation systems A

Stand-alone operation B

Migrating from S5-H to S7-400H C

Differences between fault-tolerant systems and standard systems D

Function modules and communication processors supported by the S7-400H E

Connection examples for redundant I/Os F

05/2008
A5E00267695-04

Safety Guidelines

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

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

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

⚠CAUTION
with a safety alert symbol, indicates that minor personal injury can result if proper precautions are not taken.

CAUTION
without a safety alert symbol, indicates that property damage can result if proper precautions are not taken.

NOTICE
indicates that an unintended result or situation can occur if the corresponding information is not taken into account.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The device/system may only be set up and used in conjunction with this documentation. Commissioning and operation of a device/system may only be performed by **qualified personnel**. Within the context of the safety notes in this documentation qualified persons are defined as persons who are authorized to commission, ground and label devices, systems and circuits in accordance with established safety practices and standards.

Prescribed Usage

Note the following:

⚠WARNING
This device 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. Correct, reliable operation of the product requires proper transport, storage, positioning and assembly as well as careful operation and maintenance.

Trademarks

All names identified by ® are registered trademarks of the Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

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

Siemens AG
Industry Sector
Postfach 48 48
90327 NÜRNBERG
GERMANY

Ordernumber: A5E00267695-034
Ⓟ 05/2008

Table of contents

1 Preface 15

1.1 Preface 15

2 Fault-tolerant automation systems 21

2.1 Redundant automation systems in the SIMATIC series 21

2.2 Increasing system availability 23

3 S7-400H installation options 25

3.1 S7-400H installation options 25

3.2 Rules for the assembly of fault-tolerant stations 27

3.3 The S7–400H base system 28

3.4 I/O modules for S7–400H 30

3.5 Communication 31

3.6 Tools for configuration and programming 32

3.7 The user program 33

3.8 Documentation 34

4 Getting started 35

4.1 Getting started 35

4.2 Requirements 35

4.3 Hardware installation and S7-400H commissioning 36

4.4 Examples of the reaction of the fault-tolerant system to faults 38

5 Installation of a CPU 41x–H 39

5.1 Control and display elements of the CPUs 39

5.2 Monitoring functions of the CPU 44

5.3 Status and error displays 46

5.4 Mode selector switch 49

5.5 Security levels 50

5.6 Operating sequence for memory reset 51

5.7 Structure and Functions of the Memory Cards 54

5.8 Multipoint interface (MPI) 57

5.9 PROFIBUS DP interface 58

5.10 Overview of the parameters for the S7-400H CPUs 59

6 Special functions of a CPU 41x-H ... 61
- 6.1 Updating the firmware without a memory card ... 61
- 6.2 Firmware update in RUN mode ... 63
- 6.3 Reading service data ... 65

7 S7–400H in PROFIBUS DP mode ... 67
- 7.1 CPU 41x–H as PROFIBUS DP master ... 67
- 7.1.1 DP address areas of 41xH CPUs ... 68
- 7.1.2 CPU 41xH as PROFIBUS DP master ... 68
- 7.1.3 Diagnostics of a 41xH CPU operating as PROFIBUS DP master ... 71
- 7.2 Consistent Data ... 76
- 7.2.1 Consistency of communication blocks and functions ... 77
- 7.2.2 Access to the CPU RAM ... 77
- 7.2.3 Consistency rules for SFB 14 "GET" or reading tag and SFB 15 "PUT" or writing tag ... 78
- 7.2.4 Reading data consistently from a DP standard slave and writing consistently to a DP standard slave ... 79
- 7.2.5 Consistent data access without using SFC 14 or SFC 15 ... 80

8 System and operating states of the S7–400H ... 83
- 8.1 System and operating states of the S7–400H ... 83
- 8.2 Introduction ... 84
- 8.3 The system states of the S7-400H ... 87
- 8.4 The operating states of the CPUs ... 88
- 8.4.1 STOP operating state ... 89
- 8.4.2 STARTUP operating state ... 90
- 8.4.3 LINK-UP and UPDATE operating states ... 90
- 8.4.4 RUN operating state ... 91
- 8.4.5 HOLD operating state ... 92
- 8.4.6 TROUBLESHOOTING operating state ... 92
- 8.5 Self-test ... 94
- 8.6 Time-based reaction ... 97
- 8.7 Evaluation of process interrupts in the S7-400H system ... 97

9 Link-up and update ... 99
- 9.1 Effects of link-up and updating ... 99
- 9.2 Conditions for link-up and update ... 100
- 9.3 Link-up and update ... 101
- 9.3.1 Link-up sequence ... 105
- 9.3.2 Update sequence ... 107
- 9.3.3 Switch to CPU with modified configuration or expanded memory configuration ... 110
- 9.3.4 Disabling link-up and update ... 113
- 9.4 Time monitoring ... 114
- 9.4.1 Time-based reaction ... 117
- 9.4.2 Determining the monitoring times ... 118
- 9.4.3 Performance values for link-up and update ... 125
- 9.4.4 Influences on time-based reaction ... 126
- 9.5 Special features in link-up and update operations ... 127

10 Using I/Os in S7–400H 129
10.1 Using I/Os in S7–400H 129
10.2 Introduction 129
10.3 Using single-channel, one-sided I/Os 131
10.4 Using single-channel switched I/Os 133
10.5 Connecting redundant I/Os 138
10.5.1 Connecting redundant I/Os 138
10.5.2 Signal modules for redundancy 146
10.5.3 Evaluating the passivation status 163
10.6 Other options for connecting redundant I/Os 164
11 Communication 169
11.1 Communication 169
11.2 Fundamentals and basic concepts 170
11.3 Usable networks 173
11.4 Usable communication services 173
11.5 Communications via fault-tolerant S7 connections 174
11.5.1 Communication between fault-tolerant systems 176
11.5.2 Communication between fault-tolerant systems and a fault-tolerant CPU 179
11.5.3 Communication between fault-tolerant systems and PCs 180
11.6 Communication via S7 connections 182
11.6.1 Communication via S7 connections - one-sided mode 183
11.6.2 Communication via redundant S7 connections 185
11.6.3 Communication via a point-to-point CP on the ET 200M 186
11.6.4 Custom linking to single-channel systems 187
11.7 Communication performance 188
11.8 General issues in communication 190
12 Configuring with STEP 7 193
12.1 Configuring with STEP 7 193
12.2 Configuring with STEP 7 194
12.2.1 Rules for the assembly of fault-tolerant stations 195
12.2.2 Configuring hardware 196
12.2.3 Assigning parameters to modules in a fault-tolerant station 196
12.2.4 Recommendations for setting the CPU parameters 197
12.2.5 Configuring networking 198
12.3 Programming device functions in STEP 7 199

13 Failure and replacement of components during operation 201

13.1 Failure and replacement of components during operation 201

13.2 Failure and replacement of components during operation 202
13.2.1 Failure and replacement of a CPU 202
13.2.2 Failure and replacement of a power supply module 204
13.2.3 Failure and replacement of an input/output or function module 205
13.2.4 Failure and replacement of a communication module 207
13.2.5 Failure and replacement of a synchronization module or fiber-optic cable 208
13.2.6 Failure and replacement of an IM 460 and IM 461 interface module 212

13.3 Failure and replacement of components of the distributed I/Os 213
13.3.1 Failure and replacement of a PROFIBUS-DP master 214
13.3.2 Failure and replacement of a redundant PROFIBUS-DP interface module 215
13.3.3 Failure and replacement of a PROFIBUS-DP slave 216
13.3.4 Failure and replacement of PROFIBUS-DP cables 217

14 System modifications in operation 219

14.1 System modifications in operation 219

14.2 Possible hardware modifications 220

14.3 Adding components in PCS 7 225
14.3.1 PCS 7, step 1: Modification of hardware 227
14.3.2 PCS 7, Step 2: Offline modification of the hardware configuration 228
14.3.3 PCS 7, Step 3: Stopping the standby CPU 228
14.3.4 PCS 7, Step 4: Loading new hardware configuration in the standby CPU 229
14.3.5 PCS 7, Step 5: Switch to CPU with modified configuration 230
14.3.6 PCS 7, Step 6: Transition to redundant state 231
14.3.7 PCS 7, Step 7: Editing and downloading the user program 232
14.3.8 Adding interface modules in PCS 7 233

14.4 Removing components in PCS 7 234
14.4.1 PCS 7, step I: Offline modification of the hardware configuration 236
14.4.2 PCS 7, step II: Editing and downloading the user program 237
14.4.3 PCS 7, step III: Stopping the standby CPU 238
14.4.4 PCS 7, step IV: Loading new hardware configuration in the standby CPU 238
14.4.5 PCS 7, step V: Switch to CPU with modified configuration 239
14.4.6 PCS 7, step VI: Transition to redundant state 240
14.4.7 PCS 7, step VII: Modification of hardware 241
14.4.8 Removing interface modules in PCS 7 242

14.5 Adding components in STEP 7 243
14.5.1 STEP 7, Stepp 1: Adding hardware 245
14.5.2 STEP 7, step 2: Offline modification of the hardware configuration 246
14.5.3 STEP 7, step 3: Expanding and downloading OBs 246
14.5.4 STEP 7, step 4: Stopping the standby CPU 247
14.5.5 STEP 7, step 5: Loading new hardware configuration in the standby CPU 247
14.5.6 STEP 7, step 6: Switch to CPU with modified configuration 248
14.5.7 STEP 7, step 7: Transition to redundant state 249
14.5.8 STEP 7, step 8: Editing and downloading the user program 250
14.5.9 Adding interface modules in STEP 7 251

14.6 Removing components in STEP 7 252
14.6.1 STEP 7, step I: Offline modification of the hardware configuration 253
14.6.2 STEP 7, step II: Editing and downloading the user program 254
14.6.3 STEP 7, step III: Stopping the standby CPU 254
14.6.4 STEP 7, step IV: Loading new hardware configuration in the standby CPU 255
14.6.5 STEP 7, step V: Switch to CPU with modified configuration 256
14.6.6 STEP 7, step VI: Transition to redundant state 257
14.6.7 STEP 7, step VII: Modification of hardware 258
14.6.8 STEP 7, step VIII: Editing and downloading organization blocks 258
14.6.9 Removing interface modules in STEP 7 259

14.7 Editing CPU parameters 260
14.7.1 Editing CPU parameters 260
14.7.2 Step A: Editing CPU parameters offline 262
14.7.3 Step B: Stopping the standby CPU 262
14.7.4 Step C: Loading new hardware configuration in the standby CPU 263
14.7.5 Step D: Switch to CPU with modified configuration 264
14.7.6 Step E: Transition to redundant state 265

14.8 Changing the CPU memory configuration 266
14.8.1 Changing the CPU memory configuration 266
14.8.2 Expanding load memory 266
14.8.3 Changing the type of load memory 268

14.9 Reconfiguration of a module 271
14.9.1 Reconfiguration of a module 271
14.9.2 Step A: Editing parameters offline 273
14.9.3 Step B: Stopping the standby CPU 274
14.9.4 Step C: Loading new hardware configuration in the standby CPU 274
14.9.5 Step D: Switch to CPU with modified configuration 275
14.9.6 Step E: Transition to redundant state 277

15 Synchronization modules 279

15.1 Synchronization modules for S7–400H 279

15.2 Installation of fiber-optic cables 283

15.3 Selecting fiber-optic cables 285

16 S7-400 cycle and reaction times 291

16.1 Cycle time 292

16.2 Calculating the cycle time 294

16.3 Different cycle times 299

16.4 Communication load 301

16.5 Reaction time 304

16.6 Calculating cycle and reaction times 310

16.7 Examples of calculating the cycle and reaction times 311

16.8 Interrupt reaction time 314

16.9 Example of calculation of the interrupt reaction time 316

16.10 Reproducibility of delay and watchdog interrupts 317

17 **Technical data** ... 319

17.1 Technical specifications of the CPU 412–3H; (6ES7412 3HJ14 0AB0) ... 319

17.2 Technical specifications of the CPU 414–4H; (6ES7414-4HM14-0AB0) ... 327

17.3 Technical specifications of the CPU 417–4H; (6ES7417-4HT14-0AB0) ... 336

17.4 Technical specifications of the memory cards ... 345

17.5 Runtimes of the FCs and FBs for redundant I/Os ... 346

A **Characteristic values of redundant automation systems** ... 349

A.1 Basic concepts ... 349

A.2 Comparison of MTBF for selected configurations ... 354
A.2.1 System configurations with centralized I/Os ... 354
A.2.2 System configurations with distributed I/Os ... 356
A.2.3 Comparison of system configurations with standard and fault-tolerant communication ... 359

B **Stand-alone operation** ... 361

C **Migrating from S5-H to S7-400H** ... 367

C.1 General aspects ... 367

C.2 Configuration, programming and diagnostics ... 368

D **Differences between fault-tolerant systems and standard systems** ... 369

E **Function modules and communication processors supported by the S7-400H** ... 373

F Connection examples for redundant I/Os ... 375
F.1 SM 321; DI 16 x DC 24 V, 6ES7321–1BH02–0AA0 ... 375
F.2 SM 321; DI 32 x DC 24 V, 6ES7321–1BL00–0AA0 ... 376
F.3 SM 321; DI 16 x AC 120/230V, 6ES7321–1FH00–0AA0 ... 377
F.4 SM 321; DI 8 x AC 120/230 V, 6ES7321–1FF01–0AA0 ... 378
F.5 SM 321; DI 16 x DC 24V, 6ES7321–7BH00–0AB0 ... 379
F.6 SM 321; DI 16 x DC 24V, 6ES7321–7BH01–0AB0 ... 380
F.7 SM 326; DO 10 x DC 24V/2A, 6ES7326–2BF01–0AB0 ... 381
F.8 SM 326; DI 8 x NAMUR, 6ES7326–1RF00–0AB0 ... 382
F.9 SM 326; DI 24 x DC 24 V, 6ES7326–1BK00–0AB0 ... 383
F.10 SM 421; DI 32 x UC 120 V, 6ES7421–1EL00–0AA0 ... 384
F.11 SM 421; DI 16 x DC 24 V, 6ES7421–7BH01–0AB0 ... 385
F.12 SM 421; DI 32 x DC 24 V, 6ES7421–1BL00–0AB0 ... 386
F.13 SM 421; DI 32 x DC 24 V, 6ES7421–1BL01–0AB0 ... 387
F.14 SM 322; DO 8 x DC 24 V/2 A, 6ES7322–1BF01–0AA0 ... 388
F.15 SM 322; DO 32 x DC 24 V/0,5 A, 6ES7322–1BL00–0AA0 ... 389
F.16 SM 322; DO 8 x AC 230 V/2 A, 6ES7322–1FF01–0AA0 ... 390
F.17 SM 322; DO 4 x DC 24 V/10 mA [EEx ib], 6ES7322–5SD00–0AB0 ... 391
F.18 SM 322; DO 4 x DC 15 V/20 mA [EEx ib], 6ES7322–5RD00–0AB0 ... 392
F.19 SM 322; DO 8 x DC 24 V/0,5 A, 6ES7322–8BF00–0AB0 ... 393
F.20 SM 322; DO 16 x DC 24 V/0,5 A, 6ES7322–8BH01–0AB0 ... 394
F.21 SM 332; AO 8 x 12 bit, 6ES7332–5HF00–0AB0 ... 395
F.22 SM 332; AO 4 x 0/4...20 mA [EEx ib], 6ES7332–5RD00–0AB0 ... 396
F.23 SM 422; DO 16 x AC 120/230 V/2 A, 6ES7422–1FH00–0AA0 ... 397
F.24 SM 422; DO 32 x DC 24 V/0,5 A, 6ES7422–7BL00–0AB0 ... 398
F.25 SM 331; AI 4 x 15 Bit [EEx ib]; 6ES7331–7RD00–0AB0 ... 399
F.26 SM 331; AI 8 x 12 Bit, 6ES7331–7KF02–0AB0 ... 400
F.27 SM 331; AI 8 x 16 Bit; 6ES7331–7NF00–0AB0 ... 401
F.28 SM 331; AI 8 x 16 Bit; 6ES7331–7NF10–0AB0 ... 402
F.29 AI 6xTC 16Bit iso, 6ES7331-7PE10-0AB0 ... 403
F.30 SM 331; AI 8 x 0/4...20mA HART, 6ES7331-7TF01-0AB0 ... 404
F.31 SM 332; AO 4 x 12 bit; 6ES7332–5HD01–0AB0 ... 406
F.32 SM 332; AO 8 x 0/4...20mA HART, 6ES7332-8TF01-0AB0 ... 407
F.33 SM 431; AI 16 x 16 bit, 6ES7431–7QH00–0AB0 ... 408
Glossary ... 409
Index ... 413

Tables

Table 5-1	LEDs on the CPUs	41
Table 5-2	Mode selector switch settings	49
Table 5-3	Levels of protection of a CPU	50
Table 5-4	Types of memory card	55
Table 7-1	41x CPUs, MPI/DP interface as PROFIBUS DP	68
Table 7-2	Meaning of the "BUSF" LED of the 41x CPU operating as DP master	71
Table 7-3	Reading out the diagnostics information with STEP 7	72
Table 7-4	Event detection of the CPU 41xH as a DP master	75
Table 8-1	Overview of S7-400H system states	87
Table 8-2	Causes of error leading to redundancy loss	91
Table 8-3	Reaction to errors during the self-test	94
Table 8-4	Reaction to a recurring comparison error	95
Table 8-5	Reaction to checksum errors	95
Table 8-6	Hardware fault with one-sided call of OB 121, checksum error, second occurrence	96
Table 9-1	Properties of link-up and update functions	99
Table 9-2	Conditions for link-up and update	100
Table 9-3	Typical values for the user program part	125
Table 10-1	Interfaces for the use of single-channel switched I/O	133
Table 10-2	Signal modules for redundancy	146
Table 10-3	Interconnecting digital output modules with/without diodes	155
Table 10-4	Analog input modules and encoders	160
Table 10-5	Example of redundant I/O, OB1 part	167
Table 10-6	Example of redundant I/O, OB 122 part	168
Table 10-7	For the monitoring times I/O used redundantly	168
Table 14-1	Modifiable CPU parameters	260
Table 15-1	Accessory fiber-optic cable	285
Table 15-2	Specification of fiber-optic cables for indoor applications	286
Table 15-3	Specification of fiber-optic cables for outdoor applications	288
Table 16-1	Cyclic program execution	292
Table 16-2	Factors influencing cycle time	294
Table 16-3	Allocation of the process image transfer time, CPU 412-3H	295
Table 16-4	Portion of the process image transfer time, CPU 414–4H	296
Table 16-5	Portion of the process image transfer time, CPU 417-4H	297
Table 16-6	Extension of the cycle time	297
Table 16-7	Operating system execution time at the scan cycle checkpoint	298

Table 16-8 Cycle time extension due to nested interrupts 298
Table 16-9 Direct access of the CPUs to I/O modules 308
Table 16-10 Direct access of the CPUs to I/O modules in the expansion unit with local link 308
Table 16-11 Direct access of the CPUs to I/O modules in the expansion unit with remote link 309
Table 16-12 Example of calculating the reaction time 310
Table 16-13 Process and interrupt reaction times; maximum interrupt reaction time without communication 314
Table 16-14 Reproducibility of time-delay and cyclic interrupts of the CPUs 317
Table 17-1 Runtimes of the blocks for redundant I/Os 346

Figures

Figure 2-1	Operating objectives of redundant automation systems	21
Figure 2-2	Totally integrated automation solutions with SIMATIC	23
Figure 2-3	Example of redundancy in a network without an error or fault	24
Figure 2-4	Example of redundancy in a 1-of-2 system with error/fault	24
Figure 2-5	Example of redundancy in a 1-out-of-2 system with total failure	24
Figure 3-1	Overview	26
Figure 3-2	Hardware of the S7–400H base system	28
Figure 3-3	User documentation for fault-tolerant systems	34
Figure 4-1	Hardware installation	36
Figure 5-1	Arrangement of the operator controls and displays on the CPU 412-3H	39
Figure 5-2	Layout of the control and display elements of the CPU 414-4H/417-4H	40
Figure 5-3	Jack	42
Figure 5-4	Mode selector switch settings	49
Figure 5-5	Design of the memory card	54
Figure 7-1	Diagnostics with CPU 41xH	73
Figure 7-2	Diagnostic addresses for DP master and DP slave	74
Figure 7-3	DP slave properties	81
Figure 8-1	Synchronizing the subsystems	85
Figure 8-2	System and operating modes of the fault-tolerant system	88
Figure 9-1	Sequence of link-up and update	102
Figure 9-2	Update sequence	103
Figure 9-3	Example of minimum signal duration of an input signal during the update	104
Figure 9-4	Meanings of the times relevant for updates	115
Figure 9-5	Correlation between the minimum I/O hold time and the maximum disable time for priority classes > 15	119
Figure 10-1	Single-channel, switched ET 200M distributed I/O	134
Figure 10-2	Redundant I/O in central and expansion units	138
Figure 10-3	Redundant I/O in the one-sided DP slave	139
Figure 10-4	Redundant I/O in the switched DP slave	140
Figure 10-5	Redundant I/O in single mode	141
Figure 10-6	Fault-tolerant digital input module in 1-out-of-2 configuration with one encoder	153
Figure 10-7	Fault-tolerant digital input modules in 1-out-of-2 configuration with two encoders	154
Figure 10-8	Fault-tolerant digital output modules in 1-out-of-2 configuration	154
Figure 10-9	Fault-tolerant analog input modules in 1-out-of-2 configuration with one encoder	156
Figure 10-10	Fault-tolerant analog input modules in 1-out-of-2 structure with two encoders	160
Figure 10-11	Fault-tolerant analog output modules in 1-out-of-2 configuration	161

Figure 10-12	Redundant one-sided and switched I/O	164
Figure 10-13	Flow chart for OB1	166
Figure 11-1	Example of an S7 connection	171
Figure 11-2	Example of how number of resulting subconnections depends on the configuration	172
Figure 11-3	Example of redundancy with fault-tolerant system and redundant ring	176
Figure 11-4	Example of redundancy with fault-tolerant system and redundant bus system	177
Figure 11-5	Example of fault-tolerant system with additional CP redundancy	177
Figure 11-6	Example of redundancy with fault-tolerant system and fault-tolerant CPU	179
Figure 11-7	Example of redundancy with fault-tolerant system and redundant bus system	180
Figure 11-8	Example of redundancy with a fault-tolerant system, redundant bus system, and CP redundancy on PC.	181
Figure 11-9	Example of linking of standard and fault-tolerant systems to a redundant ring	183
Figure 11-10	Example of linking standard and fault-tolerant systems to a redundant bus system	184
Figure 11-11	Example of redundancy with fault-tolerant systems and a redundant bus system with redundant standard connections	185
Figure 11-12	Example of linking of a fault-tolerant system and a single-channel third-party system	186
Figure 11-13	Example of linking of a fault-tolerant system to a single-channel external system	187
Figure 11-14	Communication load as a variable of data throughput (basic profile)	188
Figure 11-15	Communication load as a function of the response time (basic profile)	189
Figure 15-1	Synchronization module	280
Figure 15-2	Fiber-optic cables, installation using distribution boxes	289
Figure 16-1	Elements and composition of the cycle time	293
Figure 16-2	Different cycle times	299
Figure 16-3	Minimum cycle time	300
Figure 16-4	Formula: Influence of communication load	301
Figure 16-5	Distribution of a time slice	301
Figure 16-6	Dependency of the cycle time on the communication load	303
Figure 16-7	DP cycle times on the PROFIBUS DP network	305
Figure 16-8	Shortest reaction time	306
Figure 16-9	Longest reaction time	307
Figure A-1	MDT	350
Figure A-2	MTBF	351
Figure A-3	Common Cause Failure (CCF)	352
Figure A-4	Availability	353
Figure B-1	Overview: System structure for system modifications during operation	365
Figure F-1	Example of an interconnection with SM 321; DI 16 x DC 24 V	375
Figure F-2	Example of an interconnection with SM 321; DI 32 x DC 24 V	376

Figure F-3 Example of an interconnection with SM 321; DI 16 x AC 120/230 V 377
Figure F-4 Example of an interconnection with SM 321; DI 8 x AC 120/230 V 378
Figure F-5 Example of an interconnection with SM 321; DI 16 x DC 24V 379
Figure F-6 Example of an interconnection with SM 321; DI 16 x DC 24V 380
Figure F-7 Example of an interconnection with SM 326; DO 10 x DC 24 V/2 A 381
Figure F-8 Example of an interconnection with SM 326; DI 8 x NAMUR 382
Figure F-9 Example of an interconnection with SM 326; DI 24 x DC 24 V 383
Figure F-10 Example of an interconnection with SM 421; DI 32 x UC 120 V 384
Figure F-11 Example of an interconnection with SM 421; DI 16 x 24 V 385
Figure F-12 Example of an interconnection with SM 421; DI 32 x 24 V 386
Figure F-13 Example of an interconnection with SM 421; DI 32 x 24 V 387
Figure F-14 Example of an interconnection with SM 322; DO 8 x DC 24 V/2 A 388
Figure F-15 Example of an interconnection with SM 322; DO 32 x DC 24 V/0.5 A 389
Figure F-16 Example of an interconnection with SM 322; DO 8 x AC 230 V/2 A 390
Figure F-17 Example of an interconnection with SM 322; DO 16 x DC 24 V/10 mA [EEx ib] 391
Figure F-18 Example of an interconnection with SM 322; DO 16 x DC 15 V/20 mA [EEx ib] 392
Figure F-19 Example of an interconnection with SM 322; DO 8 x DC 24 V/0.5 A 393
Figure F-20 Example of an interconnection with SM 322; DO 16 x DC 24 V/0.5 A 394
Figure F-21 Example of an interconnection with SM 332, AO 8 x 12 bit 395
Figure F-22 Example of an interconnection with SM 332; AO 4 x 0/4...20 mA [EEx ib] 396
Figure F-23 Example of an interconnection with SM 422; DO 16 x 120/230 V/2 A 397
Figure F-24 Example of an interconnection with SM 422; DO 32 x DC 24 V/0.5 A 398
Figure F-25 Example of an interconnection with SM 331, AI 4 x 15 bit [EEx ib] 399
Figure F-26 Example of an interconnection with SM 331; AI 8 x 12 bit 400
Figure F-27 Example of an interconnection with SM 331; AI 8 x 16 bit 401
Figure F-28 Example of an interconnection with SM 331; AI 8 x 16 bit 402
Figure F-29 Example of an interconnection AI 6xTC 16Bit iso 403
Figure F-30 Interconnection example 1 SM 331; AI 8 x 0/4...20mA HART 404
Figure F-31 Interconnection example 2 SM 331; AI 8 x 0/4...20mA HART 405
Figure F-32 Example of an interconnection with SM 332, AO 4 x 12 bit 406
Figure F-33 Interconnection example 3 SM 332; AO 8 x 0/4...20mA HART 407
Figure F-34 Example of an interconnection with SM 431; AI 16 x 16 bit 408

Preface 1

1.1 Preface

Purpose of the manual

This manual represents a useful reference and contains information on operating options, functions and technical specifications of the S7-400H CPUs.

For information on installing and wiring those and other modules to install an S7-400H system, refer to the *S7-400 Programmable Controllers, Installation* manual.

Basic knowledge required

A general knowledge of automation technology is considered essential for the understanding of this manual.

We presume that the readership has sufficient knowledge of computers or equipment similar to a PC, such as programming devices, running under the operating system Windows 2000 or XP. An S7-400H is configured using the STEP 7 basic software, and you should thus be familiar in the handling of this software. This knowledge is provided in the *Programming with STEP 7* manual.

In particular when operating an S7-400H system in safety-relevant areas, you should always observe the information on the safety of electronic control systems provided in the appendix of the *S7-400 Automation System, Hardware and Installation* manual.

Validity of the manual

The manual is relevant to the following components:

- CPU 412–3H; 6ES7412–3HJ14–0AB0 with firmware version V4.5.0 or higher
- CPU 414–4H; 6ES7414–4HM14–0AB0 with firmware version V4.5.0 or higher
- CPU 417–4H; 6ES7417–4HT14–0AB0 with firmware version V4.5.0 or higher

Versions required or order numbers of essential system components

System component	Version required or order number
External master on PROFIBUS DP CP 443-5 Extended	Order no. 6GK7443–5DX03–0XE0 hardware version 1 or higher, and firmware version 5.1.4 or higher
	Order no. 6GK7443–5DX04–0XE0 hardware version 1 or higher, and firmware version 6.4.0 or higher
Communication module CP 443–1 (Industrial Ethernet, TCP / ISO transport)	6GK7443–1EX10–0XE0, hardware version 1 or higher, and firmware version 2.6.7 or higher
	6GK7443–1EX11–0XE0, hardware version 1 or higher, and firmware version 2.6.7 or higher
Communication module CP 443–5 Basic (PROFIBUS; S7 communication)	6GK7443–5FX02–0XE0 hardware version 2 or higher, and firmware version 3.2 or higher

Note

There may be further restriction for various modules. Refer to the information in the corresponding product information and FAQs, or in SIMATIC NET News.

Installing the STEP 7 hardware update

In addition to STEP 7, you also need a hardware update. You can download the update files directly from the STEP 7 pages on the Internet. You can do this in "STEP 7 -> Configuring Hardware" with the "Options -> Install Hardware Updates" menu command.

Certification

For details on certifications and standards, refer to the *S7-400 Programmable Controllers, Module Data* manual, section 1.1, Standards and Certifications.

Online help

In addition to the manual, you will find detailed support on how to use the software in the integrated online help system of the software.

The help system can be accessed using various interfaces:

- The **Help** menu contains several commands: **Contents** opens the Help index. You will find help on H systems in **Configuring H-Systems**.
- **Using Help** provides detailed instructions on using the online help system.
- The context-sensitive help system provides information on the current context, for example, on an open dialog box or an active window. You can call this help by clicking "Help" or using the F1 key.
- The status bar provides a further form of context-sensitive help. It shows a short description of each menu command when you position the mouse pointer over a command.
- A short info text is also shown for the toolbar buttons when you hold the mouse pointer briefly over a button.

If you prefer to read the information of the online help in printed form, you can print individual topics, books or the entire help system.

Finding your way

The manual contains various features supporting quick access to specific information:

- At the beginning of the manual you will find a complete table of contents.
- The left column on each page of the sections provides an overview of the contents of each section.
- The appendix is followed by a glossary which defines important specialist terminology used in this manual.
- At the end of the manual, you will find a comprehensive index that allows quick access to information on specific subjects.

Recycling and disposal

The S7-400H system contains environmentally compatible materials and can be recycled. To recycle and dispose of your old device in an environmentally friendly way, please contact a company certified to deal with electronic waste.

Additional support

If you have any questions relating to the products described in this manual, and do not find the answers in this documentation, please contact your Siemens partner at our local offices.

You will find information on who to contact at:

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

A guide to the technical documents for the various SIMATIC products and systems is available at:

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

You will find the online catalog and order system at:

http://mall.ad.siemens.com/

H/F Competence Center

The H/F Competence Center in Nuremberg offers a special workshop
on the topic of fault-tolerant SIMATIC S7 automation systems.
The H/F Competence Center also offers configuration and commissioning support,
and help in finding solutions for problems in your plant.
Phone: +49 (911) 895-4759
Fax: +49 (911) 895-5193
E-mail: hf-cc.aud@siemens.com

Training center

We offer a range of courses to help you to get started with the SIMATIC S7 automation system. Please contact your regional Training Center, or the Central Training Center in Nuremberg, 90327 Germany. Telephone: +49 (911) 895–3200
Internet: http://www.sitrain.com

A&D Technical Support

Worldwide, available 24 hours a day:

Worldwide (Nuremberg) Technical support		
Local time: 24 hours a day, 365 days a year Telephone: +49 (0) 180 5050-222 Fax: +49 (0) 180 5050-223 E-mail: adsupport@siemens.com GMT: +1:00		
Europe / Africa (Nuremberg) **Authorization**	**United States (Johnson City)** **Technical Support and Authorization**	**Asia / Australia (Peking)** **Technical Support and Authorization**
Local time: Mon. - Fri. 8:00 a.m. to 5:00 p.m. Telephone: +49 (0) 180 5050-222 Fax: +49 (0) 180 5050-223 E-mail: adsupport@siemens.com GMT: +1:00	Local time: Mon. - Fri. 8:00 a.m. to 5:00 p.m. Telephone: +1 (423) 262 2522 Fax: +1 (423) 262 2289 E-mail: simatic.hotline@sea.siemens.com GMT: -5:00	Local time: Mon. - Fri. 8:00 a.m. to 5:00 p.m. Telephone: +86 10 64 75 75 75 Fax: +86 10 64 74 74 74 E-mail: adsupport.asia@siemens.com GMT: +8:00
German and English are spoken on the Technical Support and Authorization hotline.		

Service & Support on the Internet

In addition to the information in our documentation, you can also access our knowledge base online at:

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

There you will find:

- The newsletter, which constantly provides you with up-to-date information on your products.
- The right documentation for you using our Service & Support search engine.
- A forum, where users and experts from all over the world exchange their experiences.
- Your local Industry Automation and Drive Technology representative.
- Information on field service, repairs, spare parts and consulting.

Fault-tolerant automation systems 2

2.1 Redundant automation systems in the SIMATIC series

Operating objectives of redundant automation systems

Redundant automation systems are used in practice with the aim of achieving a higher degree of availability or fault tolerance.

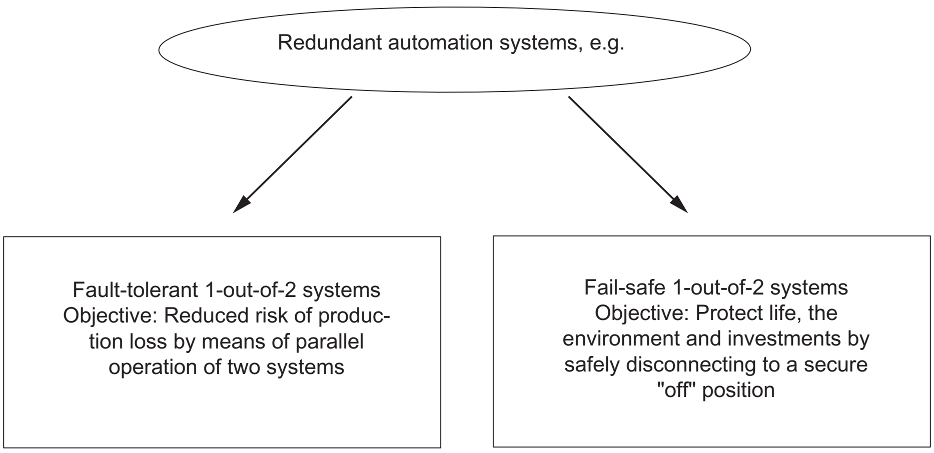


Figure 2-1 Operating objectives of redundant automation systems

Note the difference between fault-tolerant and fail-safe systems.
An S7-400H is a fault-tolerant automation system that may only be used to control safety-relevant processes in conjunction with additional measures.

Why fault-tolerant automation systems?

The purpose of using fault-tolerant automation systems is to reduce production downtimes, regardless of whether the failures are caused by an error/fault or are due to maintenance work.

The higher the costs of downtimes, the greater the need to use a fault-tolerant system. The generally higher investment costs of fault-tolerant systems are soon returned by the avoiding loss of production.

Software redundancy

For many applications, the requirements for redundancy quality or the extent of plant sections that may require redundant automation systems do not necessarily justify the implementation of a special fault-tolerant system. Usually, simple software mechanisms are adequate to allow a failed control task to be continued on a substitute system if a problem occurs.

The optional "SIMATIC S7 Software Redundancy" software package can be implemented on S7-300 and S7-400 standard systems to control processes that tolerate failover delays to a substitute system in the seconds range, such as water works, water treatment systems or traffic flows.

Redundant I/O

Input/output modules are termed redundant when they exist twice and they are configured and operated as redundant pairs. The use of redundant I/O provides the highest degree of availability, because the system tolerates the failure of a CPU or of a signal module. If you require a redundant I/O, you use the blocks of the "Functional I/O Redundancy" block library, see section Connecting redundant I/Os (Page 138).

2.2 Increasing system availability

The S7-400H automation system satisfies the high demands on availability, intelligence and distribution put on state-of-the-art automation systems. The system provides all functionality required for the acquisition and preparation of process data, including functions for the open-loop and closed-loop control and monitoring of assemblies and plants.

Totally integrated systems

The S7-400H automation system and all other SIMATIC components, such as the SIMATIC PCS 7 control system, are harmonized. The totally integrated system, ranging from the control room to the sensors and actuators, is implemented as a matter of course and guarantees maximum system performance.

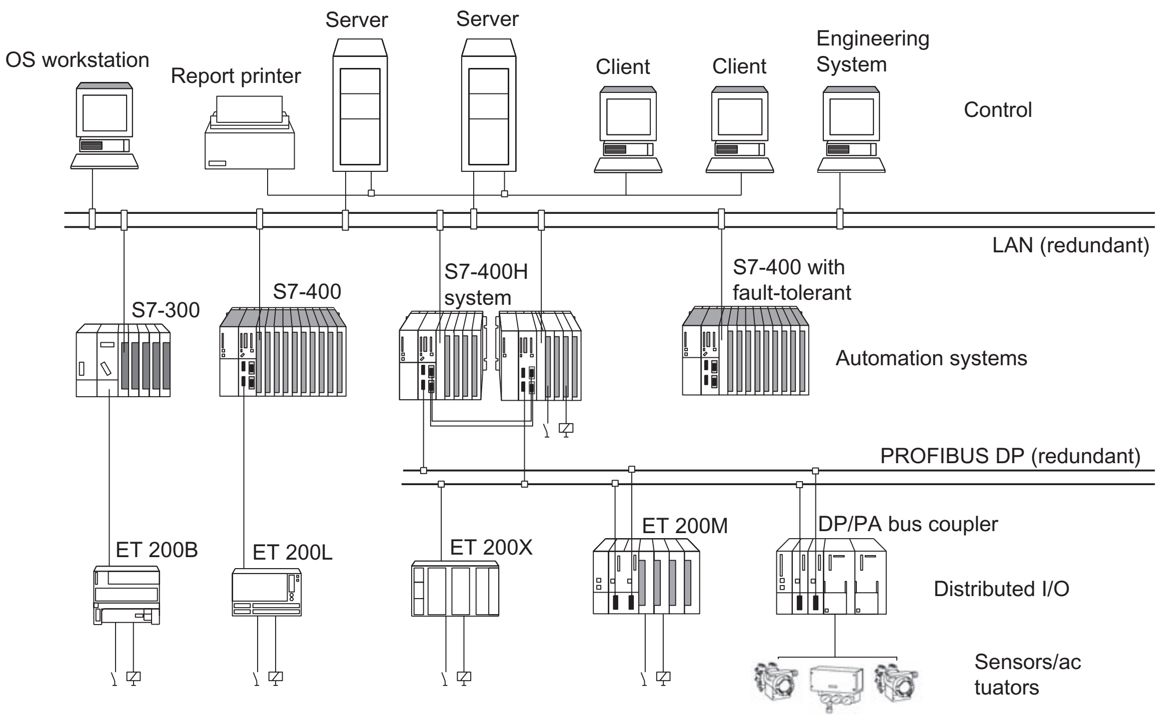


Figure 2-2 Totally integrated automation solutions with SIMATIC

Graduated availability by duplicating components

The redundant structure of the S7-400H ensures availability at all times. This means all essential components are duplicated.

This redundant structure includes the CPUs, the power supply modules, and the hardware for linking the two CPUs.

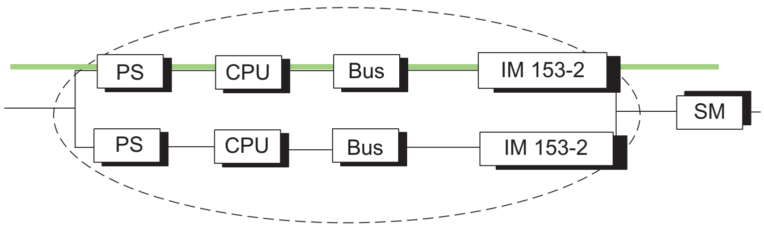
You yourself decide on any other components you want to duplicate to increase availability depending on the specific process you are automating.

Redundancy nodes

Redundant nodes represent the reliability of systems with redundant components in case of failure. A redundant node can be considered as independent when the failure of a component within the node does not result in reliability constraints in other nodes or in the entire system.

The availability of the entire system can be illustrated simply based on a block diagram. With a 1-out-of-2 system, **one** component of the redundant node may fail without impairing the operability of the overall system. The weakest link in the chain of redundant nodes determines the availability of the overall system

No error/fault



Redundant nodes with 1-of-2 redundancy

Figure 2-3 Example of redundancy in a network without an error or fault

With error/fault

The following figure shows how a component may fail without impairing the functionality of the overall system.

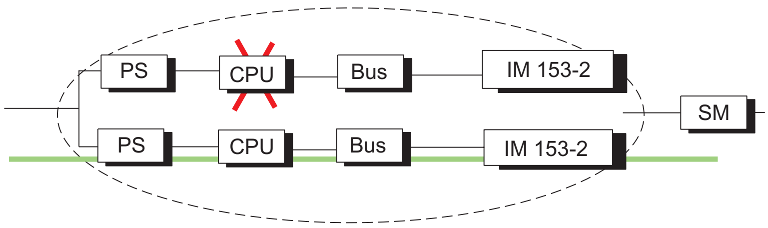
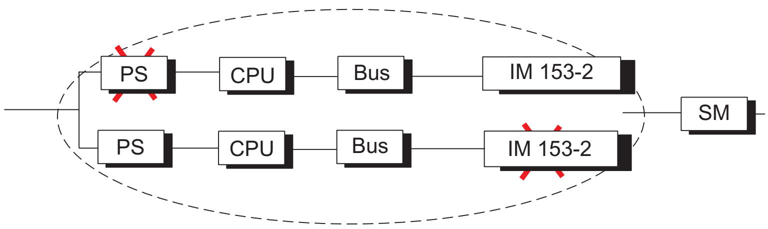


Figure 2-4 Example of redundancy in a 1-of-2 system with error/fault

Failure of a redundancy node (total failure)

The following figure shows that the system is no longer operable, because both subunits have failed in a 1-of-2 redundancy node (total failure).



Redundant nodes with 1-of-2 redundancy

Figure 2-5 Example of redundancy in a 1-out-of-2 system with total failure

S7-400H installation options 3

3.1 S7-400H installation options

The first part of the description deals with the basic configuration of the redundant S7-400H automation system, and with the components of an S7-400H base system. We then set out the hardware components with which you can expand this base system.

The second part deals with the software tools which you are going to use to configure and program the S7-400H. Included is a description of the add-on and extended functions available for the S7-400 base system which you need to create the user program, and to utilize all the properties of your S7-400H in order to increase availability.

Important information on the configuration

WARNING
Open equipment S7–400 modules are classified as open equipment, meaning you must install the S7-400 in a cubicle, cabinet or switch room which can only be accessed by means of a key or tool. Such cubicles, cabinets or switch rooms may only be accessed by instructed or authorized personnel.

The following figure shows an example of an S7-400H configuration with shared distributed I/O and connection to a redundant plant bus. The next pages deal with the hardware and software components required for the installation and operation of the S7-400H.

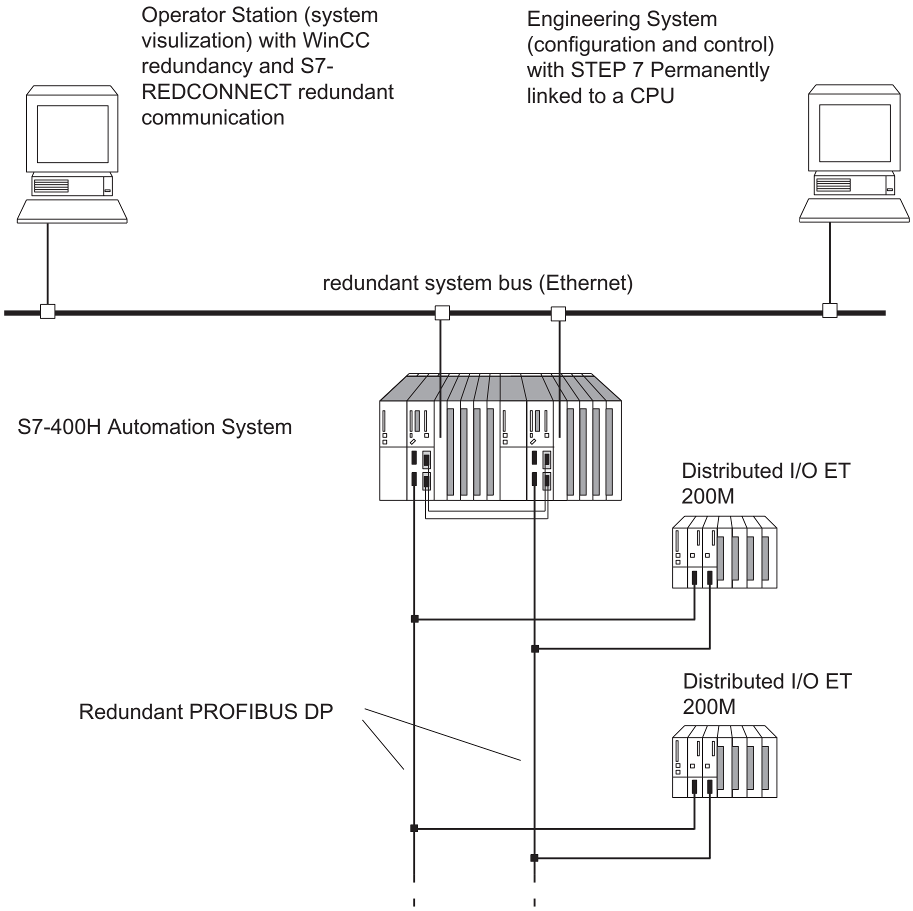


Figure 3-1 Overview

Further information

The components of the S7-400 standard system are also used in the fault-tolerant S7–400H automation system. For a detailed description of all hardware components for S7–400, refer to the reference manual *S7-400 automation system module specifications*.

The rules governing the design of the user program and the use of components laid down for the S7-400 standard system also apply to the fault-tolerant S7-400H automation system. Refer to the descriptions in the *Programming with STEP 7* manual, and to the *System Software for S7-300/400; Standard and System Functions* reference manual.

3.2 Rules for the assembly of fault-tolerant stations

The following rules have to be complied with for a fault-tolerant station, in addition to the rules that generally apply to the arrangement of modules in the S7-400:

- The CPUs always have to be inserted in the same slots.
- Redundantly used external DP master interfaces or communication modules must be inserted in the same slots in each case.
- External DP master interface modules for redundant DP master systems should only be inserted in central racks, rather than in expansion racks.
- Redundantly used modules (for example, CPU 417-4H, DP slave interface module IM 153-2) must be identical, i.e. they must have the same order number, the same version, and the same firmware version.

3.3 The S7–400H base system

Hardware of the base system

The base system consists of the hardware components required for a fault-tolerant control. The following figure shows the components in the configuration.

The base system may be expanded with the standard modules of an S7-400. Restrictions only apply to the function and communications modules; see Appendix Function modules and communication processors supported by the S7-400H (Page 373).

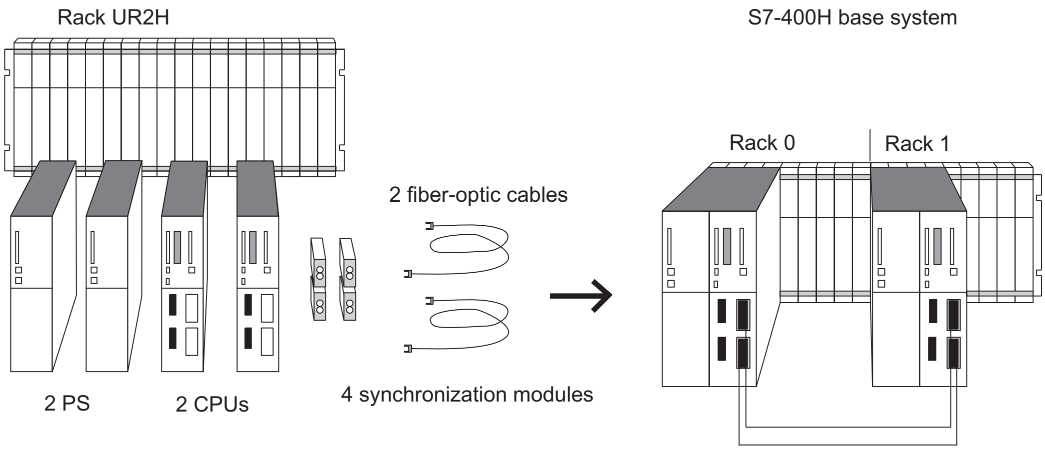


Figure 3-2 Hardware of the S7–400H base system

Central modules

The two central modules are the heart of the S7-400H. Use the switch on the rear of the CPU to set the rack numbers. In the following sections, we will refer to the CPU in rack 0 as CPU 0, and to the CPU in rack 1 as CPU 1.

Rack for S7–400H

The UR2-H rack supports the installation of two separate subsystems with nine slots each, and is suitable for installation in 19" cabinets.

You can also set up the S7-400H in two separate racks. Racks UR1 and UR2 are available for this purpose.

Power supply

You require one power supply module from the standard range of the S7-400 for each fault-tolerant CPU, or to be more precise, for each of the two subsystems of the S7-400H.

The power supply modules available have rated input voltages of 24 V DC and 120/230 V AC, at an output current of 10 and 20 A.

To increase availability of the power supply, you can also use two redundant power supplies in each subsystem. For this configuration, you should use the PS 407 10 A R power supply module for rated voltages of 120/230 V AC and an output current of 10 A.

Synchronization modules

The synchronization modules are used to link the two CPUs. They are installed in the CPUs and interconnected by means of fiber-optic cables.

There are two types of synchronization modules: one for distances up to 10 meters, and one for distances up to 10 km between the CPUs.

A fault-tolerant system requires 4 synchronization modules of the same type. For more information on synchronization modules, refer to section Synchronization modules for S7–400H (Page 279).

Fiber-optic cables

The fiber-optic cables are used to interconnect the synchronization modules for the redundant link between the two central modules. They interconnect the upper and two lower pairs of synchronization modules.

You will find the specifications of fiber-optic cables suitable for use in an S7-400H is in section Selecting fiber-optic cables (Page 285).

3.4 I/O modules for S7–400H

The S7-400H can be equipped with I/O modules of the SIMATIC S7 series. The I/Os can be used in the following devices:

- Central devices
- Expansion devices
- Distributed on PROFIBUS DP.

You will find the function modules (FMs) and communications modules (CPs) suitable for use in the S7-400H in Appendix Function modules and communication processors supported by the S7-400H (Page 373).

Versions of the I/O configuration

Versions for the configuration of I/O modules:

- Single-channel, one-sided configuration with standard availability

  With the single-channel, one-sided configuration: single input/output modules. The I/O modules are located in only one unit, and are always addressed by this unit.

  However, the CPUs are interconnected by means of redundancy coupler when operating in redundant mode and thus execute the user program identically.
- Single-channel, switched configuration with enhanced availability

  Switched single-channel distributed configurations contain only one set of the I/O modules, but they can be addressed by both units.
- Redundant dual-channel configuration with maximum availability

  A redundant dual-channel configuration contains two sets of the I/O modules which can be addressed by both units.

Further information

For detailed information on using the I/O, refer to chapter Using I/Os in S7–400H (Page 129).

3.5 Communication

The S7-400H supports the following communication methods and mechanisms:

- System buses with Industrial Ethernet
- Point-to-point connection

This equally applies to the central and distributed components you can use. Suitable communication modules are listed in appendix Function modules and communication processors supported by the S7-400H (Page 373).

Communication availability

You can vary the availability of communication with the S7-400H. The S7-400H supports various solutions to meet your communication requirements. These range from a simple linear network structure to a redundant optical two-fiber loop.

Fault-tolerant communication on PROFIBUS or Industrial Ethernet networks is supported only by the S7 communication functions.

Programming and configuring

Apart from the use of additional hardware components, there are basically no differences with regard to configuration and programming compared to standard systems. Fault-tolerant connections only have to be configured; specific programming is not necessary.

All communication functions required for fault-tolerant communication are integrated in the operating system of the fault-tolerant CPU. These functions run automatically in the background, for example, to monitor the communication connection, or to automatically change over a redundant connection in the event of error.

Further information

For detailed information on communication with the S7-400H, refer to chapter Communication (Page 169).

3.6 Tools for configuration and programming

Similar to the S7-400, the S7-400H is also configured and programmed using STEP 7.

You only need to make allowances for slight restrictions when you write the user program. However, there are some additional details specific to the fault-tolerant configuration. The operating system monitors the redundant components and automatically fails over to the standby components when an error occurs. You have already configured the relevant information and communicated it to the system in your STEP 7 program.

For detailed information, refer to the online help, to chapter Configuring with STEP 7 (Page 193) and to Appendix Differences between fault-tolerant systems and standard systems (Page 369).

Optional software

All standard tools, engineering tools and runtime software used in the S7-400 system are also supported by the S7-400H system.

3.7 The user program

The rules of designing and programming a standard S7-400 system also apply to the S7-400H.

In terms of user program execution, the S7-400H behaves in exactly the same manner as a standard system. The integral synchronization functions of the operating system are executed automatically in the background. You do not need to configure these functions in your user program.

In redundant operation, the user programs are stored identically and executed synchronously and event-driven on both CPUs.

However, we offer you various blocks which you can use to tune your program in order to improve its response to any extension of cycle times due to operations such as updates.

Specific blocks for S7–400H

In addition to the blocks supported in the S7-400 and S7-400H systems, the S7-400H software provides further blocks you can use to influence the redundancy functions.

You can react to redundancy errors of the S7-400H using the following organization blocks:

- OB 70, I/O redundancy errors
- OB 72, CPU redundancy errors

SFC 90 "H_CTRL" can be used to influence fault-tolerant systems as follows:

- You can disable link-up in the master CPU.
- You can disable updating in the master CPU.
- You can remove, resume or immediately start a test component of the cyclic self-test.

NOTICE
Required OBs Always download the following error OBs to the S7-400H CPU: OB 70, OB 72, OB 80, OB 82, OB 83, OB 85, OB 86, OB 87, OB 88, OB 121 and OB 122. If you ignore this, the fault-tolerant system changes to STOP when an error occurs.

Further information

For detailed information on programming the blocks listed above, refer to the *Programming with STEP 7* manual, and to the *System Software for S7-300/400; System and Standard Functions* reference manual.

3.8 Documentation

The diagram below provides an overview of the descriptions of the various components and options in the S7-400H automation system.

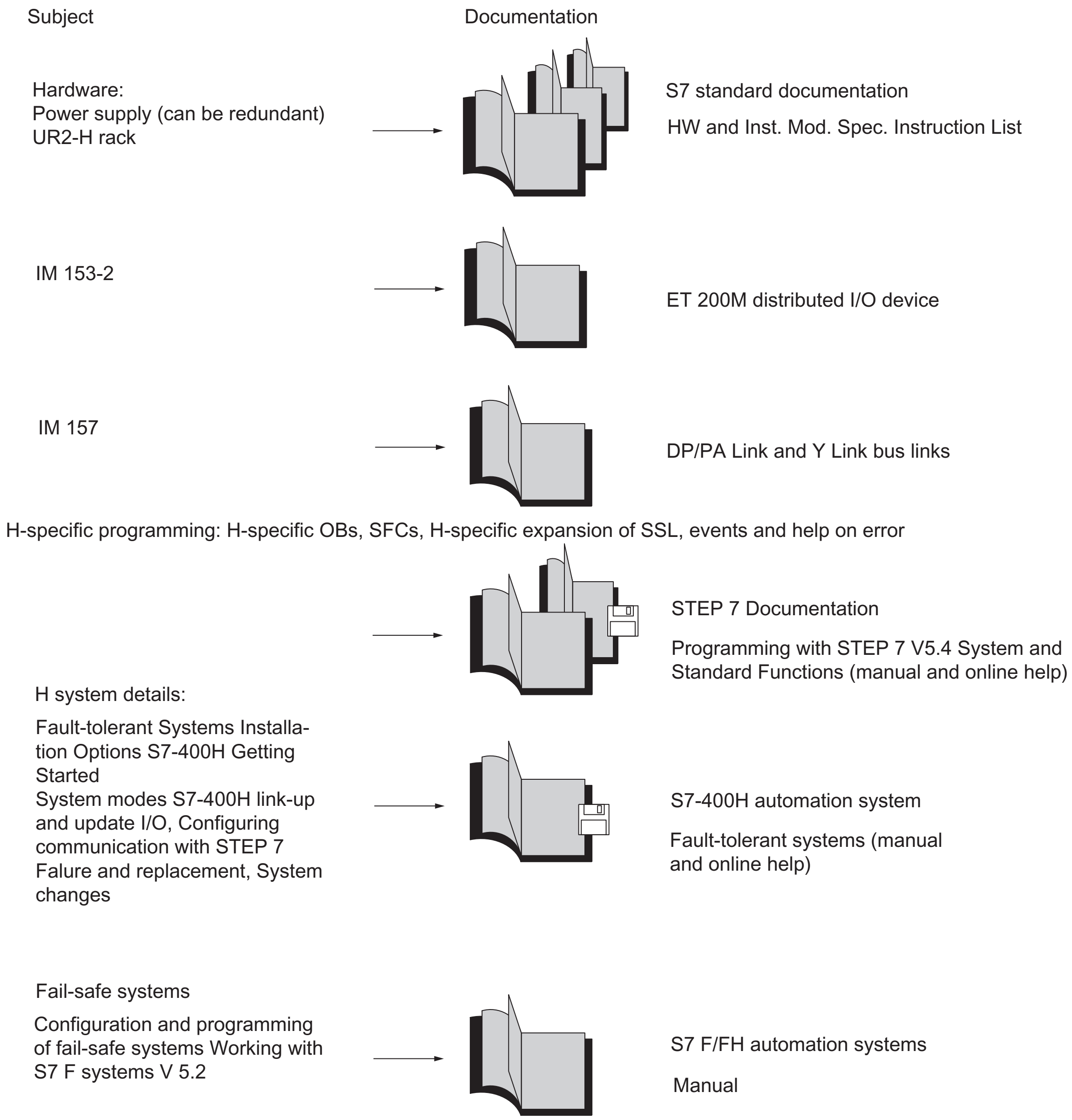


Figure 3-3 User documentation for fault-tolerant systems

4 Getting started

4.1 Getting started

This guide walks you through the steps that have to be performed to commission the system, based on a specific example and results in a working application. You will learn how an S7-400H programmable logic controller operates and become familiar with its response to a fault.

It takes about one to two hours to work through this example, depending on your previous experience.

4.2 Requirements

The following requirements must be met:

Correctly installed and valid version of the standard STEP 7 software on your programming device; see section Configuring with STEP 7 (Page 194). Any necessary hardware updates are installed.

Modules required for the hardware configuration:

- an S7-400H automation system consisting of:
  - 1 x UR2–H rack
  - 2 power supply modules, PS 407 10A
  - 2 x H–CPUs
  - 4 synchronization modules
  - 2 fiber-optic cables
- an ET 200M distributed I/O device with active backplane bus and
  - 2 IM 153-2
  - 1 digital input module, SM321 DI 16 x DC24V
  - 1 digital output module, SM322 DO 16 x DC24V
- all necessary accessories, such as PROFIBUS cables, etc.

4.3 Hardware installation and S7-400H commissioning

Installing Hardware

Follow the steps below to install the S7-400H as shown in the following figure:

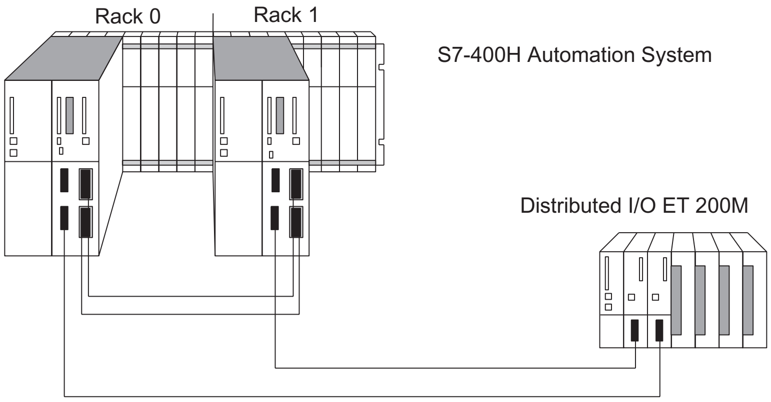


Figure 4-1 Hardware installation

1. Install both modules of the S7-400H automation system as described in the *S7-400 Automation Systems, Installation* and *Module Specifications* manuals.
2. Set the rack numbers using the switch on the rear of the CPUs.

   An incorrectly set rack number prevents online access and, under certain circumstances, the CPU will not start up.
3. Install the synchronization modules in the CPUs as described in the *S7-400 Automation System, Installation* manual.
4. Connect the fiber-optic cables.

   Always interconnect the two upper and lower synchronization modules of the CPUs. Route your fiber-optic cables so that they are safely protected against any damage.

   You should also always make sure that the two fiber-optic are cables routed separately. This increases availability, and protects the fiber-optic cables from potential double errors caused, for example, by breaking both cables at the same time.

   Always connect the fiber-optic cables to both CPUs before you switch on the power supply or the system. Otherwise both CPUs may execute the user program as master CPU.
5. Configure the distributed I/O as described in the *ET 200M Distributed I/O Device* manual.
6. Connect the programming device to the first H-CPU, CPU0. This CPU will be the master of your S7-400H.
7. A high-quality RAM test is run after POWER ON. This takes about 10 minutes. The CPU cannot be accessed and the STOP LED flashes for the duration of this test. If you use a backup battery, this test is no longer performed when you power up in future.

Commissioning the S7-400H

Follow the steps outlined below to commission the S7-400H:

1. In SIMATIC Manager, open the sample project "HProject". The configuration corresponds to the hardware configuration described in "Requirements".
2. Open the hardware configuration of the project by selecting the hardware object, right-clicking, and selecting the context menu command "Object -> Open". If your configuration matches, continue with step 6.
3. If your hardware configuration does not match the project, for example different module types, MPI addresses or DP address, edit and save the project accordingly. For further information, refer to the basic Help of SIMATIC Manager.
4. Open the user program in the "S7 program" folder.

   In the offline view, this "S7 program" folder is only assigned to CPU0. The user program is executable with the described hardware configuration. It activates the LEDs on the digital output module.
5. Edit the user program as necessary to adapt it to your hardware configuration, and then save it.
6. Select "PLC -> Download" to download the user program to CPU0.
7. Start up the S7-400H automation system by setting the mode selector switch of CPU0 to RUN and then the switch on CPU1. The CPU performs a warm restart and calls OB100.

   Result: CPU0 starts up as the master CPU and CPU1 as the standby CPU. After the standby CPU is linked and updated, your S7-400H assumes the redundant mode and executes the user program. It activates the LEDs on the digital output module.

Note

You can also start and stop the S7-400H automation system using STEP 7.

For further information, refer to the online help.

You can only initiate a cold start using the PG command "Cold start". Before you can do this, the CPU must be in STOP mode and the mode selector switch must be set to RUN. OB102 is called in the cold start routine.

4.4 Examples of the reaction of the fault-tolerant system to faults

Example 1: Failure of a CPU or of a power supply module

Initial situation: The S7-400H is in redundant mode.

1. Simulate a CPU0 failure by turning off the power supply.

   Result: The LEDs REDF, IFM1F and IFM2F light up on CPU1. CPU1 goes into single mode and continues to process the user program.

2. Turn the power supply back on.

   Result:

   – CPU0 performs an automatic LINK-UP and UPDATE.

   – CPU0 changes to RUN, and now operates in standby mode.

   – The S7-400H is in redundant mode.

Example 2: Failure of a fiber-optic cable

Initial situation: The S7-400H is in redundant mode. The mode selector switch of each CPU is set to RUN.

1. Disconnect one of the fiber-optic cables.

   Result: The LEDs REDF and IFM1F or IFM2F (depending on which fiber-optic cable was disconnected) now light up on both CPUs. The standby CPU changes to the TROUBLESHOOTING mode. The other CPU remains master and continues operation in single mode.

2. Reconnect the fiber-optic cable.

   Result: The standby CPU performs starts a LINK-UP and UPDATE. The S7-400H resumes redundant mode.

Installation of a CPU 41x–H 5

5.1 Control and display elements of the CPUs

Operator controls and displays on the CPU 412-3H

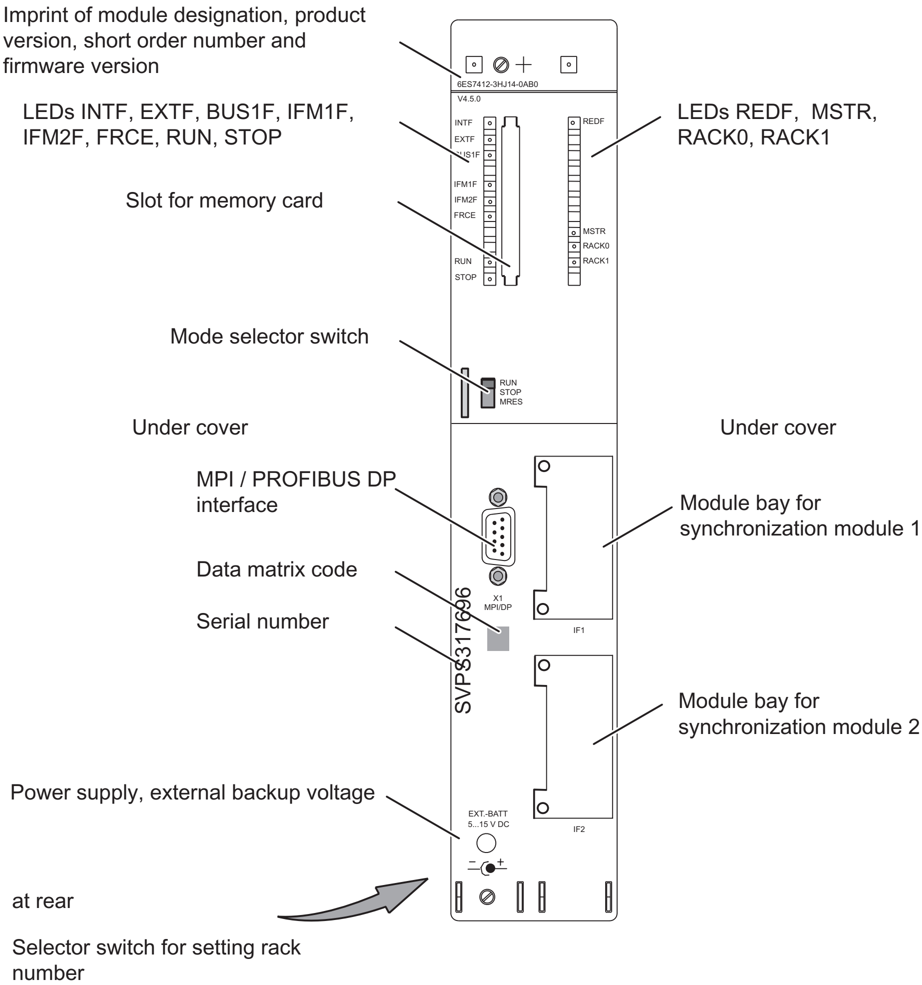


Figure 5-1 Arrangement of the operator controls and displays on the CPU 412-3H

Control and display elements of CPU 414–4H/417–4H

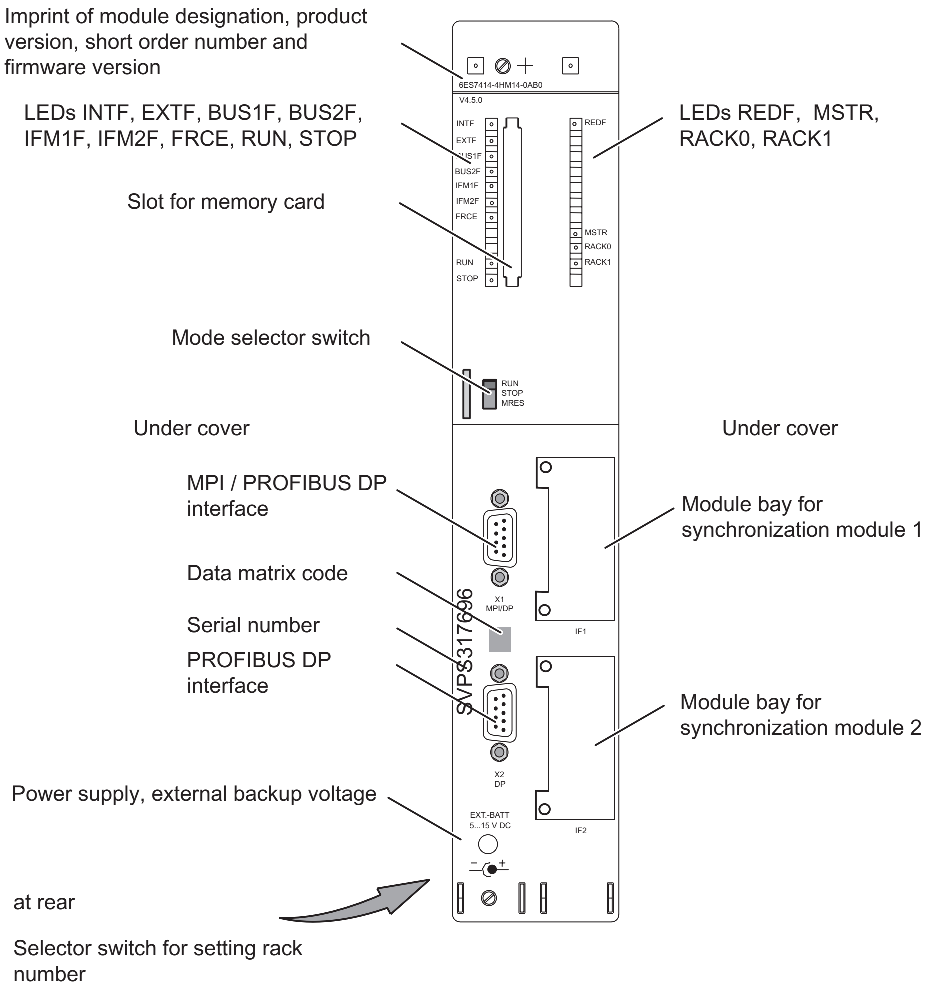


Figure 5-2 Layout of the control and display elements of the CPU 414-4H/417-4H

LED displays

The following shows you an overview of the LEDs on the individual CPUs.

Sections Monitoring functions of the CPU (Page 44) and Status and error displays (Page 46) describe the states and errors/faults indicated by these LEDs.

Table 5-1 LEDs on the CPUs

LED	Color	Meaning
INTF	Red	Internal error
EXTF	Red	External error
FRCE	Yellow	Active force request
RUN	Green	RUN mode
STOP	Yellow	STOP mode
BUS1F	Red	Bus fault on MPI/PROFIBUS DP interface 1
BUS2F	Red	Bus fault on PROFIBUS DP interface 2
MSTR	Yellow	CPU controls the process
REDF	Red	Redundancy loss/fault
RACK0	Yellow	CPU in rack 0
RACK1	Yellow	CPU in rack 1
IFM1F	Red	Error in synchronization module 1
IFM2F	Red	Error in synchronization module 2

Mode selector switch

You can use the mode selector switch to set the current mode of the CPU. The mode selector switch is a rocker switch with three positions.

Section Mode selector switch (Page 49) describes the functions of the mode selector switch.

Memory card slot

You can insert a memory card into this slot.

There are two types of memory card:

- RAM cards

  You can expand the CPU loading memory with the RAM card.
- Flash cards

  A FLASH card can be used for fail-safe backup of the user program and data without a backup battery. You can program the flash card either on the programming device or in the CPU. The flash card also expands the load memory of the CPU.

  For detailed information on memory cards, refer to section Structure and Functions of the Memory Cards (Page 54).

Slot for interface modules

You can insert an H-Sync module in this slot.

MPI/DP interface

You can, for example, connect the following devices to the MPI interface of the CPU:

- Programming devices
- Operator control and monitoring devices
- Further S7-400 or S7-300 controllers, see section Multipoint interface (MPI) (Page 57).

Use the bus connection connector with the oblique cable outlet, see the *S7–400 Automation System, Hardware and Installation* manual.

The MPI interface can also be configured for operation as DP master and therefore as a PROFIBUS DP interface with up to 32 DP slaves.

PROFIBUS DP interface

The PROFIBUS DP interface supports the connection of distributed I/O, PGs and OPs.

Setting the rack number

Use the selector switch on the rear panel of the CPU to set the rack number. The switch has two positions: 1 (up) and 0 (down). One CPU is allocated rack number 0, and the partner CPU is assigned rack number 1. The default setting of all CPUs is rack number 0.

Connecting an external backup voltage to the "EXT. BATT." socket

The S7-400H power supply modules support the use of two backup batteries. This allows you to:

- Back up the user program stored in RAM.
- Retain bit memory, timers, counters, system data and data in dynamic data blocks.
- Back up the internal clock.

You can achieve the same backup by connecting a DC voltage between 5 V DC and 15 V DC to the "EXT. BATT." socket of the CPU.

Properties of the "EXT. BATT." input:

- Polarity reversal protection
- Short-circuit current limiting to 20 mA

To connect an auxiliary voltage to the "EXT. BATT" input, you require a cable with a 2.5 mm ∅ plug as shown in the figure below. Observe the polarity of the jack.

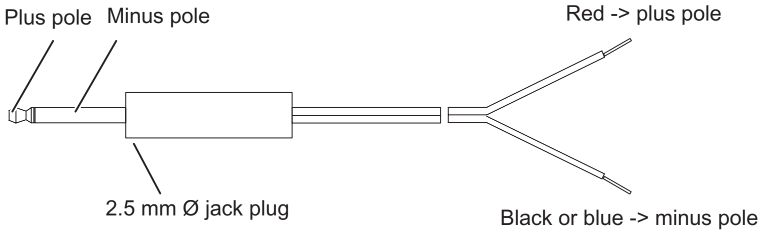


Figure 5-3 Jack

You can order a jack plug with an assembled cable from the using order number A5E00728552A.

Note

When you replace a power supply module and want to backup the user program and data stored in RAM while doing so, you should connect an auxiliary power supply to the "EXT. BATT." input as mentioned earlier.

5.2 Monitoring functions of the CPU

Monitoring functions and error messages

The hardware and operating system of the CPU provide monitoring functions to ensure proper operation and defined reactions to errors. Various errors may also trigger a reaction in the user program.

The table below provides an overview of possible errors and their causes, and the corresponding reactions of the CPU.

Additional testing and information functions are available on each CPU and can be called in STEP 7.

Error class	Cause of error	Reaction of the operating system	Error LED
Access error	Module failure (SM, FM, CP)	LED "EXTF" remains lit until the error is eliminated. In SMs: • Call of OB122 • Entry in the diagnostics buffer • In the case of input modules: Entry of "null" for the date in the accumulator or the process image In the case of other modules: • Call of OB122	EXTF
Timeout error	• The user program execution time (OB1 and all interrupt and error OBs) exceeds the specified maximum cycle time. • OB request error • Overflow of the start information buffer • Time-of-day error interrupt	LED "INTF" remains lit until the error is eliminated. Call of OB80. If the OB is not loaded: CPU goes into STOP mode.	INTF
Power supply module(s) fault (not line power failure)	In the central or expansion rack: • at least one backup battery in the power supply module is flat. • the backup voltage is missing. • the 24 V supply to the power supply module has failed.	Call of OB 81 If the OB is not loaded: The CPU remains in RUN.	EXTF
Diagnostic interrupt	An I/O module which supports interrupts reports a diagnostics interrupt.	Call of OB 82 If the OB is not loaded: CPU goes into STOP mode.	EXTF
Removal/insertion interrupt	Removal or insertion of an SM, and insertion of a wrong module type.	Call of OB 83 If the OB is not loaded: CPU goes into STOP mode.	EXTF
CPU hardware fault	• A memory error was detected and eliminated • Redundant link: Data transfer errors.	Call of OB 84 If the OB is not loaded: The CPU remains in RUN.	INTF
Program execution error	• Priority class is called, but the corresponding OB is not available. • In the case of an SFB call: missing or faulty instance DB	Call of OB 85 If the OB is not loaded: CPU goes into STOP mode.	INTF

Error class	Cause of error	Reaction of the operating system	Error LED
	• Process image update error		EXTF
Failure of a rack/station	• Power failure in an expansion rack • Failure of a DP segment • Failure of a coupling segment: missing or defective IM, interrupted cable	Call of OB 86 If the OB is not loaded: CPU goes into STOP mode.	EXTF
Execution canceled	Execution of a program block was canceled. Possible reasons for the cancellation are: • Nesting depth of parenthesis above maximum • Nesting depth of master control relay above maximum • Nesting depth of synchronization errors above maximum • Nesting depth of block calls (U stack) above maximum • Nesting depth of block calls (B stack) above maximum • Error allocating local data	Call of OB 88 If the OB is not loaded: CPU goes into STOP mode.	INTF
Programming error	User program error: • BCD conversion error • Range length error • Range error • Alignment error • Write error • Timer number error • Counter number error • Block number error • Block not loaded	Call of OB 121 If the OB is not loaded: CPU goes into STOP mode.	INTF
MC7 code error	Error in the compiled user program, for example, illegal OP code or a jump beyond block end	CPU goes into STOP mode. Restart or CPU memory reset required.	INTF

5.3 Status and error displays

RUN and STOP LEDs

The RUN and STOP LEDs provide information about the active CPU operating status.

LED		Meaning
RUN	STOP	
H	D	CPU is in RUN mode.
D	H	CPU is in STOP mode. The user program is not executed. Cold restart/ warm restart is possible. If the STOP status was triggered by an error, the error indicator (INTF or EXTF) is also set.
B 2 Hz	B 2 Hz	CPU is DEFECTIVE. All other LEDs also flash at 2 Hz.
B 0.5 Hz	H	HOLD status has been triggered by a test function.
B 2 Hz	H	A cold restart / warm restart was initiated. The cold/warm restart may take a minute or longer, depending on the length of the called OB. If the CPU still does not change to RUN, there might be an error in the system configuration.
D	B 2 Hz	Self-test with unbuffered POWER ON is busy. The self-test may take up to 10 minutes CPU memory reset is busy
x	B 0.5 Hz	The CPU requests a memory reset.
B 0.5 Hz	B 0.5 Hz	Troubleshooting mode

D = LED unlit; H = LED lit; B = LED flashing at specified frequency; x = LED status is irrelevant

MSTR, RACK0 and RACK1 LEDs

The three LEDs, MSTR, RACK0 and RACK1 provide information about the rack number set on the CPU and show which CPU controls the switched I/O.

LED			Meaning
MSTR	RACK0	RACK1	
H	x	x	CPU controls switched I/O
x	H	D	CPU on rack number 0
x	D	H	CPU on rack number 1

D = LED unlit; H = LED lit; x = LED status is irrelevant

INTF, EXTF and FRCE LEDs

The three LEDs, INTF, EXTF and FRCE, provide information about errors and special events in user program execution.

LED			Meaning
INTF	EXTF	FRCE	
H	x	x	An internal error was detected (programming or parameter assignment error).
x	H	x	An external error was detected (in other words, an error whose cause is not on the CPU module).
x	x	H	A force request is active.

H = LED lit; x = LED status is irrelevant

BUSF1 and BUSF2 LEDs

The BUSF1 and BUSF2 LEDs indicate errors on the MPI/DP and PROFIBUS DP interfaces.

LED		Meaning
BUS1F	BUS2F	
H	x	An error was found on the MPI/DP interface.
x	H	An error was found on the PROFIBUS DP interface.
B	x	DP master: One or more slaves on the PROFIBUS DP interface 1 is not responding. DP slave: Not addressed by the DP master.
x	B	DP master: One or more slaves on the PROFIBUS DP interface 2 is not responding. DP slave: Not addressed by the DP master.

H = LED lit; B = LED flashing; x = LED status is irrelevant

IFM1F and IFM2F LEDs

The IFM1F and IFM2F LEDs indicate errors on the first or second synchronization module.

LED		Meaning
IFM1F	IFM2F	
H	x	An error was detected on synchronization module 1.
x	H	An error was detected on synchronization module 2

H = LED lit; x = LED status is irrelevant

REDF LED

The REDF LED indicates specific system states and redundancy errors.

REDF LED	System state	Constraints
B 0.5 Hz	Link-up	-
B 2 Hz	Update	-
D	Redundant (CPUs are redundant)	No redundancy error
H	Redundant (CPUs are redundant)	There is an I/O redundancy error: • Failure of a DP master, or partial or total failure of a DP master system • Loss of redundancy on the DP slave

D = LED is unlit; L = LED lights up; F = LED flashes at the specified frequency

Diagnostic buffer

In STEP 7, you can select "PLC -> Module Information" to read the cause of an error from the diagnostic buffer.

5.4 Mode selector switch

Function of the mode selector switch

This switch can be used to set the CPU to RUN and STOP modes, or to reset the CPU memory. STEP 7 offers further options of changing the mode.

Positions

The mode selector switch is a rocker switch. The following figure shows all the possible positions of the mode selector.

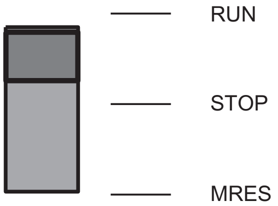


Figure 5-4 Mode selector switch settings

The following table explains the settings for the mode selector. If an error or a startup problem occurs, the CPU will either change to or stay in STOP mode regardless of the position of the mode selector switch.

Table 5-2 Mode selector switch settings

Setting	Explanations
RUN	If there is no startup problem or error and the CPU was able to switch to RUN, the CPU either runs the user program or remains idle. The I/O can be accessed.
STOP	The CPU does not execute the user program. In the default parameter setting, the output modules are disabled.
MRES (CPU memory reset; master reset)	Toggle switch position for CPU memory reset, see section Operating sequence for memory reset (Page 51)

5.5 Security levels

You can define a security level for your project in order to prevent unauthorized access to the CPU programs. The objective of these security settings is to grant a user access to specific programming device functions which are not protected by password, and to allow that user to execute those functions on the CPU. When logged on with password, the user may execute all PG functions.

Setting security levels

You can set the CPU security levels 1 to 3 in STEP 7 under "Configure Hardware".

If you do not know the password, you can clear the security setting by means of a manual CPU memory reset using the mode selector switch. The CPU must not contain a Flash card when you perform such an operation.

The following table lists the levels of protection of an S7–400 CPU.

Table 5-3 Levels of protection of a CPU

CPU function	Level of protection 1	Level of protection 2	Level of protection 3
Block list display	Access granted	Access granted	Access granted
Monitoring tags	Access granted	Access granted	Access granted
Module status STACKS	Access granted	Access granted	Access granted
Operator control and monitoring functions	Access granted	Access granted	Access granted
S7 communication	Access granted	Access granted	Access granted
Reading the time	Access granted	Access granted	Access granted
Setting the time	Access granted	Access granted	Access granted
Status block	Access granted	Access granted	Password required
Upload to PG	Access granted	Access granted	Password required
Download to CPU	Access granted	Password required	Password required
Deleting blocks	Access granted	Password required	Password required
Compressing memory	Access granted	Password required	Password required
Download user program to memory card	Access granted	Password required	Password required
Controlling selection	Access granted	Password required	Password required
Controlling tags	Access granted	Password required	Password required
Breakpoint	Access granted	Password required	Password required
Clear breakpoint	Access granted	Password required	Password required
CPU memory reset	Access granted	Password required	Password required
Force	Access granted	Password required	Password required
Updating the firmware without a memory card	Access granted	Password required	Password required

Setting the security class with SFC 109 "PROTECT"

SFC 109 "PROTECT" is used to switch between security classes 1 and 2.

5.6 Operating sequence for memory reset

Case A: You want to download a new user program to the CPU.

1. Set the switch to the STOP position.

   Result: The STOP LED is lit.
2. Toggle the switch to MRES, and hold it in that position. This mode selector switch position has a pushbutton action contact.

   Result: The STOP LED is switched off for one second, on for one second, off for one second and then remains on.
3. Then release the switch, return it to MRES within the next three seconds, and then release it again.

   Result: The STOP LED flashes for at least 3 seconds at 2 Hz (memory is reset) and then remains lit.

Case B: The STOP LED flashing slowly at 0.5 Hz indicates that the CPU is requesting a memory reset (system memory reset request, e.g. after a memory card has been removed or inserted).

Toggle the switch to MRES, and then release it again.

Result: The STOP LED flashes for at least 3 seconds at 2 Hz, the memory reset is executed and the LED then remains lit.

What happens in the CPU during a memory reset

When you run a memory reset, the following process occurs on the CPU:

- The CPU deletes the entire user program in the main memory.
- The CPU deletes the user program from the load memory. This process deletes the program from the on-board RAM and from any RAM Card. The user program elements stored on a flash card will not be deleted if you have expanded the load memory with such a card.
- The CPU resets all counters. Memory markers and timers, but not the time of day.
- The CPU tests its hardware.
- The CPU sets its parameters to default settings.
- If a flash card is inserted, the CPU copies the user program and the system parameters stored on the flash card into main memory after the memory reset.

Data retained after a memory reset...

The following values are retained after a memory reset:

- The content of the diagnostics buffer

  If you did not insert a flash card during memory reset, the CPU resets the capacity of the diagnostics buffer to its default setting of 120 entries, i.e. the most recent 120 entries will be retained in the diagnostics buffer.

  You can read the content of the diagnostics buffer using STEP 7.
- The MPI interface parameters. These define the MPI address and the highest MPI address. Note the special features shown in the table below.
- The time
- The status and value of the operating hours counter

Special feature: MPI parameters

The MPI parameters play an exceptional role during CPU memory reset. The table below lists the MPI parameters which are valid after a memory reset.

Memory reset ...	MPI parameters ...
with inserted flash card	... stored on the flash Card are valid
without plugged flash card	...are retained in the CPU and valid

Cold restart

- A cold restart initializes the process image, all memory markers, timers, counters and data blocks with the start values stored in load memory, regardless of whether these data were configured as being retentive or not.
- Program execution resumes with OB 1, or with OB 102 if available.

Warm restart

- A restart resets the process image and the non-retentive flags, timers, times and counters.

  Retentive memory markers, timers, counters and all data blocks retain their last valid value.
- Program execution resumes with OB 1, or with OB 101 if available.
- If the power supply is interrupted, the warm restart function is only available in backup mode.

Operating sequence for restart t/warm restart

1. Set the switch to the STOP position.

   Result: The STOP LED is lit.
2. Set the switch to RUN.

   Result: The STOP LED goes out, the RUN LED is lit.

Whether the CPU performs a restart or a hot restart is determined by its configuration.

Operating sequence for cold restart

You can only initiate a cold restart using the PG command "Cold restart". Before you can do this, the CPU must be in STOP mode and the mode selector switch must be set to RUN.

5.7 Structure and Functions of the Memory Cards

Order numbers

The order numbers for memory cards are listed in the technical specifications, see section Technical specifications of the memory cards (Page 345).

Design of a memory card

The size of a memory card corresponds to that of a PCMCIA card. It is inserted into a front-panel slot of the CPU.

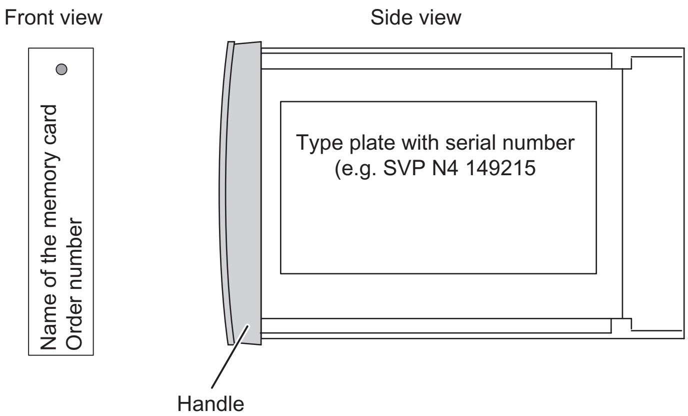


Figure 5-5 Design of the memory card

Function of the memory card

The memory card and an integrated memory section on the CPU together form the load memory of the CPU. During operation, the load memory contains the complete user program, including the comments, the symbols and special additional information that enables back-compilation of the user program as well as all module parameters.

Data stored on the memory card

The following data can be stored on memory card:

- The user program, i.e. the OBs, FBs, FCs, DBs and system data
- Parameters that determine the behavior of the CPU
- Parameters that determine the behavior of I/O modules
- The full set of project files on suitable memory cards.

Types of memory cards for the S7–400

Two types of memory card are used for the S7-400:

- RAM cards
- Flash cards

What type of memory card to use?

Whether you use a RAM card or a Flash card depends on your application.

Table 5-4 Types of memory card

If you ...	then ...
also want to be able to edit your program in RUN,	use a **RAM card**
want to keep a permanent backup of your user program on the memory card when power is off, i.e. without a backup battery or outside the CPU,	use a **Flash card**

RAM card

Insert the RAM card to download the user program to the CPU. Download the user program in STEP 7 by selecting "PLC > Download user program to Memory Card".

You can load the entire user program or individual elements such as FBs, FCs, OBs, DBs, or SDBs to the load memory when the CPU is in STOP or RUN mode.

When you remove the RAM card from the CPU, the information stored on it will be lost. The RAM card is not equipped with an integrated backup battery.

If the power supply is equipped with an operational backup battery, or the CPU is supplied with an external backup voltage at the "EXT. BATT." input, the RAM card contents are retained when power is switched off, provided the RAM card remains inserted in the CPU and the CPU remains inserted in the rack.

FLASH card

If you use a Flash card, there are two ways of loading the user program:

- Use the mode selector switch to set the CPU to STOP. Insert the FLASH card into the CPU, and then download the user program to the Flash card in STEP 7 by selecting "PLC > Download user program to Memory Card".
- Load the user program into the Flash card in offline mode on the programming device/programming adapter, and then insert the FLASH card into the CPU.

The FLASH card is a non-volatile memory, i.e. its data are retained when it is removed from the CPU or your S7-400 is being operated without backup voltage (without a backup battery in the power supply module or external backup voltage at the "EXT. BATT." input of the CPU).

You always download the full user program to a FLASH card.

Downloading additional user program elements

You can download further elements of the user program from the programming device to the integrated load memory of the CPU. Note that the content of this integrated RAM area will be deleted if the CPU performs a memory reset, i.e. load memory is updated with the user program stored on the FLASH card after a CPU memory reset.

What memory card capacity to use?

The capacity of your memory card is determined by the scope of the user program.

Determining memory requirements using SIMATIC Manager

You can view the block lengths offline by selecting the "Properties - Block folder offline" dialog box (Blocks > Object Properties > Blocks tab).

The offline view shows the following lengths:

- Size (sum of all blocks, without system data) in load memory of the PLC
- Size (sum of all blocks, without system data) in the RAM of the PLC

Block lengths on the engineering device (PG/PC) are not shown in the properties of the block container.

Block lengths are shown in "byte" units.

The following values are shown in the block properties:

- Required local data volume: Length of local data in bytes
- MC7: Length of MC7 code in bytes
- Length of DB user data
- Length in load memory of the PLC
- Length in RAM of the PLC (only if hardware assignment is known.)

The views always show these block data, regardless whether it is located in the window of an online view or of an offline view.

When a block container is opened and "View Details" is set, the project view always indicates RAM requirements, regardless of whether the block container appears in the window of an online or offline view.

You can add up the block lengths by selecting all relevant blocks. SIMATIC Manager outputs the total length of the selected blocks in its status bar.

The view does not indicate the lengths of blocks (VATs, for example) which can not be downloaded to the PLC.

Block lengths on the engineering system (PG/PC) are not shown in the Details view.

5.8 Multipoint interface (MPI)

Connectable devices

You can, for example, connect the following nodes to the MPI:

- Programming devices (PG/PC)
- Operating and monitoring devices (OPs and TDs)
- Additional SIMATIC S7 PLCs

Various compatible devices take the 24 V supply from the interface. This voltage is non-isolated.

PG/OP - CPU communication

A CPU is capable of handling several online connections to PGs/OPs in parallel. By default, one of these connections is always reserved for a PG, and one for an OP/operation and monitoring device.

CPU–CPU communication

CPUs exchange data by means of S7 communication.

For further information, refer to the *Programming with STEP 7* manual.

Connectors

Always use bus connectors with an angular cable exit for PROFIBUS DP or PG cables to connect devices to the MPI (see *Installation Manual*, Chapter 7).

MPI interface as DP interface

You can also configure the MPI interface for operation as DP interface. To do so, reconfigure the MPI interface under STEP 7 in SIMATIC Manager. This feature can be used to configure a DP segment with up to 32 slaves.

5.9 PROFIBUS DP interface

Connectable devices

You can connect any slave conforming to the DP standard to the PROFIBUS DP interface.

Here, the CPU represents the DP master, and is connected to the passive slave stations or, in stand-alone mode, to other DP masters via the PROFIBUS DP field bus.

Various compatible devices take the 24 V supply from the interface. This voltage is non-isolated.

Connectors

Always use bus connectors for PROFIBUS DP and PROFIBUS cables to connect devices to the PROFIBUS DP interface (*refer to the Installation manual*).

Redundant mode

In redundant mode, the PROFIBUS DP interfaces have the same parameters.

5.10 Overview of the parameters for the S7-400H CPUs

Default values

You can determine the CPU-specific default values by selecting "Configuring Hardware" in STEP 7.

Parameter blocks

The reactions and properties of the CPU are set at the parameters which are stored in system data blocks. The CPUs have a defined default setting. You can modify these default values by editing the parameters in the hardware configuration.

The list below provides an overview of the configurable system properties of the CPUs.

- General properties, such as the CPU name
- Startup
- Cycle/clock memory, for example the cycle monitoring time
- Retentivity, i.e. the number of memory markers, timers and counters retained
- Memory, such as local data

  Note: If you change the RAM allocation by modifying parameters, this RAM is reorganized when you download system data to the CPU. The result of this is that data blocks that were created with SFC are deleted, and the remaining data blocks are assigned initial values from the load memory.

  The RAM area available for logic and data blocks will be modified if you change the following parameter settings:

  – Size of the process image, byte-oriented in the "Cycle/Clock memory" tab
  – Communication resources in the "Memory" tab
  – Size of the diagnostic buffer in the "Diagnostics/Clock" tab
  – Number of local data for all priority classes in the "Memory" tab
- Assignment of interrupts (hardware interrupts, time delay interrupts, asynchronous error interrupts) to the priority classes
- Time-of-day interrupts, such as start, interval duration, priority
- Cyclic interrupts, for example priority, interval duration
- Diagnostics/clock, for example time-of-day synchronization
- Levels of protection
- Fault-tolerant parameters

Parameter assignment tool

You can set the individual CPU parameters using "HW Config" in STEP 7.

Note

When you modify the parameters listed below, the operating system initializes the following values:

- Size of the process input image
- Size of the process output image
- Size of the local data
- Number of diagnostic buffer entries
- Communication resources

These initializations are:

- Data blocks are initialized with the load values
- M, C, T, I, O will be deleted irrespective of the retentivity setting (0)
- DBs generated by SFC will be deleted
- Permanently configured dynamic connections will be terminated

The system starts up in the same way as with a cold restart.

Further settings

- The rack number of a fault-tolerant CPU, 0 or 1

  Use the selector switch on the rear panel of the CPU to change the rack number.
- The operating mode of a fault-tolerant CPU: Stand-alone or redundant mode

  For information on how to change the operating mode of a fault-tolerant CPU, refer to Appendix Stand-alone operation (Page 361).

6 Special functions of a CPU 41x-H

6.1 Updating the firmware without a memory card

Basic procedure

To update the firmware of a CPU, you will receive several files (*.UPD) containing the current firmware. Download these files to the CPU. You do not need a memory card to perform an online update. However, it is still possible to update the firmware using a memory card.

Requirement

The CPU whose firmware you want to update must be accessible online, for example, via PROFIBUS, MPI or Industrial Ethernet. The files containing the current firmware version must be available in the PG/PC file system. A folder may contain only the files of one firmware version. If level of protection 2 or 3 is set for the CPU, you require the password to update the firmware.

Note

You can update the firmware of the H-CPUs via Industrial Ethernet if the CPU is connected to the Industrial Ethernet via a CP. Updating the firmware over MPI can take a long time if the transfer rate is low (for example approx. 10 minutes at 187.5 Kbps)

Procedure

Proceed as follows to update the firmware of a CPU:

1. Open the station containing the CPU you want to update in HW Config.
2. Select the CPU.
3. Select the "PLC > Update Firmware" menu command.
4. In the "Update Firmware" dialog, select the path to the firmware update files (*.UPD) using the "Browse" button.

   After you have selected a file, the information in the bottom boxes of the "Update Firmware" dialog box indicate the modules for which the file is suitable and from which firmware version.
5. Click on "Run."

STEP 7 verifies that the selected file can be interpreted by the CPU and then downloads the file to the CPU. If this requires changing the operating state of the CPU, you will be asked to do this in the relevant dialog boxes.

NOTICE
Power on/off without battery backup
If the firmware update is interrupted by a power cycle without battery backup, it is possible that the CPU no longer has a functioning operating system. You can recognize this by the LEDs INTF and EXTF both flashing. You can only correct this by reloading the firmware from a memory card.

6.2 Firmware update in RUN mode

Requirement

The size of the load memory on the master and standby CPU is the same. Both sync links exist and are working.

Procedure as of STEP 7 V5.4 SP3

Follow the steps below to update the firmware of the CPUs of an H system in RUN:

1. Set one of the CPUs to STOP
2. Select this CPU in HW Config.
3. Select the "PLC > Update Firmware" menu command.

   The "Update Firmware" dialog box opens. Select the firmware file from which the current firmware will be loaded to the selected CPU.
4. In the SIMATIC Manager or in HW Config, select the "PLC > Operating Mode > Switch to CPU 41xH" and select the "with altered operating system" check box.
5. Repeat steps 1 to 3 for the other CPU.
6. Link up and update the CPUs.

Both CPUs have updated firmware (operating system) and are in redundant mode.

Procedure as of STEP 7 V5.3 SP2 up to and including STEP 7 V5.4 SP2

Follow the steps below to update the firmware of the CPUs of an H system in RUN:

1. Set one of the CPUs from the SIMATIC Manager to STOP with "PLC -> Operating Mode CPUs".
2. Select this CPU in HW Config.
3. Select the "PLC > Update Firmware" menu command.

   The "Update Firmware" dialog box opens. Select the firmware file from which the current firmware will be loaded to the selected CPU.
4. In the SIMATIC Manager or in HW Config, select the "PLC > Operating Mode > Switch to CPU 41xH" and select the "with altered operating system" check box.
5. Repeat steps 1 to 3 for the other CPU.
6. Link up and update the CPUs.

Both CPUs have updated firmware (operating system) and are in redundant mode.

NOTICE
Note the following as of STEP 7 V5.3 SP2 up to and including STEP 7 V5.4 SP2:
If you run "PLC -> Update Firmware" from HW Config with these STEP 7 versions before you have set the CPU to STOP in the SIMATIC Manager, **both** CPUs go to STOP.

Note

The third number of the firmware versions of the master and standby CPU may only differ by 1. You can only update to the newer version.

Example: From V4.5.0 to V4.5.1

Please take note of any information posted in the firmware download area.

The constraints described in section System and operating states of the S7–400H (Page 83) also apply to a firmware update in RUN

6.3 Reading service data

Use case

If you need to contact our Customer Support due to a service event, the department may require specific diagnostic information on the CPU status of your system. This information is stored in the diagnostic buffer and in the actual service data.

Select the “PLC -> Save service data” command to read this information and save the data to two files. You can then send these to Customer Support.

Please note:

- If possible, save the service data immediately after the CPU goes into STOP or the synchronization of a fault-tolerant system has been lost.
- Always save the service data of both CPUs in an H system.

Procedure

1. Select the "PLC > Save service data" command

   In the next dialog box, select the file path and the file names.
2. Save the files.
3. Forward these files to Customer Support on request.

7 S7–400H in PROFIBUS DP mode

7.1 CPU 41x–H as PROFIBUS DP master

Introduction

This chapter describes how to use the CPU as DP master and configure it for direct data exchange.

Further references

For details and information on engineering, configuring a PROFIBUS subnet and diagnostics in a PROFIBUS subnet, refer to the **STEP 7** Online Help.

Further information

For details and information on migrating from PROFIBUS DP to PROFIBUS DPV1, refer to the Internet URL:

http://support.automation.siemens.com

under article number 7027576

7.1.1 DP address areas of 41xH CPUs

Address areas of 41xH CPUs

Table 7-1 41x CPUs, MPI/DP interface as PROFIBUS DP

Address area	412-3H	414-4H	417–4H
MPI interface as PROFIBUS DP, inputs and outputs (bytes) in each case	2048	2048	2048
DP interface as PROFIBUS DP, inputs and outputs (bytes) in each case	-	6144	8192
Of those addresses you can configure up to x bytes for each I/O in the process image	-	0 to 8192	0 to 16384

DP diagnostics addresses occupy at least one byte for the DP master and each DP slave in the input address area. At these addresses, the DP standard diagnostics can be called for the relevant node by means of the LADDR parameter of SFC13, for example. Define the DP diagnostics addresses when you configure the project data. If you do not specify any DP diagnostics addresses, STEP 7 automatically assigns the addresses as DP diagnostics addresses in descending order, starting at the highest byte address.

In DPV1 master mode the slaves are usually assigned two diagnostics addresses.

7.1.2 CPU 41xH as PROFIBUS DP master

Requirements

You will need to configure the relevant CPU interface for use as a PROFIBUS DP master. i.e. make the following settings in **STEP 7**:

- Assign a network
- Configure the CPU as a PROFIBUS DP master
- Assign a PROFIBUS address
- Select the operating mode, S7-compatible or DPV1

  The default setting is DPV1
- Link DP slaves to the DP master system

Note

Is one of the PROFIBUS DP slaves a CPU 31x or CPU 41x?

If yes, you will find it in the PROFIBUS DP catalog as a ”preconfigured” station. Assign this DP slave CPU a slave diagnostic address in the PROFIBUS DP master. Link the PROFIBUS DP master to the DP slave CPU, and specify the address areas for data exchange with the DP slave CPU.

Monitor/Modify, programming via PROFIBUS

As an alternative to the MPI interface, you can use the PROFIBUS DP interface to program the CPU or execute the Monitor/Modify programming device functions.

NOTICE
The “Programming” or “Monitor/Modify” applications prolong the DP cycle if executed via the PROFIBUS DP interface.

DP master system startup

Use the following parameters to set startup monitoring of the PROFIBUS DP master:

- Ready message from module
- Parameter transfer to modules

In other words, the DP slaves must start up within the set time and be configured by the CPU (as PROFIBUS DP master).

PROFIBUS address of the PROFIBUS DP master

All PROFIBUS addresses are permissible.

Step from IEC 61158 to DPV1

The IEC 61158 standard for distributed I/Os has been enhanced. The enhancements are incorporated into IEC 61158 / IEC 61784–1:2002 Ed1 CP 3/1. The SIMATIC documentation uses the term "DPV1" in this context. The new version features various expansions and simplifications.

SIEMENS automation components feature DPV1 functionality. In order to be able to use these new features, you first have to make some modifications to your system. A full description of the migration from IEC 61158 to DPV1 is available in the FAQ section titled "Migrating from IEC 61158 to DPV1", FAQ article ID 7027576, on the Customer Support internet site.

Components supporting PROFIBUS DPV1 functionality

DPV1 master

- The S7-400 CPUs with integrated DP interface.
- CP 443-5, order number 6GK7 443–5DX03–0XE0,
  6GK7 443–5DX04–0XE0.

DPV1 slaves

- DP slaves listed in the STEP 7 hardware catalog under their family names can be identified in the information text as DPV1 slaves.
- DP slaves integrated in STEP 7 by means of GSD files revision 3 or higher.

What operating modes are there for DPV1 components?

- S7-compatible mode

  In this mode, the component is compatible with IEC 61158. However, you then cannot use the full DPV1 functionality.

- DPV1 mode

  In this mode can make full use of DPV1 functionality. Automation components in the station that do not support DPV1 can be used as before.

Compatibility between DPV1 and IEC 61158?

You can continue to use all existing slaves after converting to DPV1. These do not, however, support the enhanced functions of DPV1.

You can also use DPV1 slaves without a conversion to DPV1. In this case they behave like conventional slaves. SIEMENS DPV1 slaves can be operated in S7-compatible mode. To integrate DPV1 slaves from other manufacturers, you need a GSD file complying with IEC 61158 earlier than revision 3.

Discovering the bus topology in a DP master system using SFC103 "DP_TOPOL"

A diagnostic repeater is available to make it easier to localize disrupted modules or breaks on the DP cables when failures occur during operation. This module is a slave that discovers the topology of a DP chain and detects any problems caused by it.

You can use SFC 103 ”DP_TOPOL” to trigger the identification of the bus topology of a DP master system by the diagnostic repeater. SFC103 is described in the corresponding online help and in the *"System and Standard Functions* manual. For information on the diagnostic repeater refer to the *"Diagnostic Repeater for PROFIBUS DP* manual,
order no. 6ES7972–0AB00–8BA0.

7.1.3 Diagnostics of a 41xH CPU operating as PROFIBUS DP master

Diagnostics using LEDs

The following table shows the meaning of the BUSF LED. The BUSF LED assigned to the interface configured as the PROFIBUS DP interface always lights up or flashes when a problem occurs.

Table 7-2 Meaning of the "BUSF" LED of the 41x CPU operating as DP master

BUSF	Meaning	What to do
Off	Configuration correct; All the configured slaves are addressable	-
Lit	• DP interface error • Different Baud rates in multi-DP master operation (only in stand-alone mode)	• Evaluate the diagnosis. Reconfigure or correct the configuration.
Flashing	• Station failure	• Check whether the bus cable is connected to the CPU 41x or whether the bus is interrupted.
	• At least one of the assigned slaves is not addressable	• Wait until the 41x CPU has powered up. If the LED does not stop flashing, check the DP slaves or evaluate the diagnosis of the DP slaves.
	• Bus error (physical fault)	• Check whether the bus cable has a short-circuit or a break.

Reading out the diagnostics information with STEP 7

Table 7-3 Reading out the diagnostics information with STEP 7

DP master	Block or tab in STEP 7	Application	See ...
41x CPU	"DP slave diagnostics" tab	To display the slave diagnosis as plain text on the **STEP 7** user interface	"Hardware diagnostics" in the **STEP 7**Online Help, and the *Configuring hardware and connections with* **STEP 7** manual
	SFC 13 "DPNRM_DG"	Reading slave diagnostics data, i.e. saving them to the data area of the user program The busy bit may not be set to "0" if an error occurs while SFC 13 is being processed. You should therefore check the RET_VAL parameter whenever SFC13 was processed.	For information on the configuration of a CPU 41x, refer to the *CPU Data* reference manual; for information on the SFC, refer to the *System and Standard Functions* reference manual. For information on the configuration of other slaves, refer to the corresponding description
	SFC 59 "RD_REC"	To read out data records of the S7 diagnosis (save them to the data area of the user program)	Refer to the *System and Standard Functions reference manual*
	SFC 51 "RDSYSST"	To read out SSL sublists call SFC 51 in the diagnostics interrupt using the SSL ID W#16#00B3 and read out the SSL of the slave CPU.	
	SFB 52 "RDREC"	for DPV1 slaves Reading data records of S7 diagnostics, i.e. saving them to the data area of the user program	
	SFB 54 "RALRM"	for DPV1 slaves: To read out interrupt information within the associated interrupt OB	

Evaluating diagnostics data in the user program

The figure below shows how to evaluate the diagnostics data in the user program.

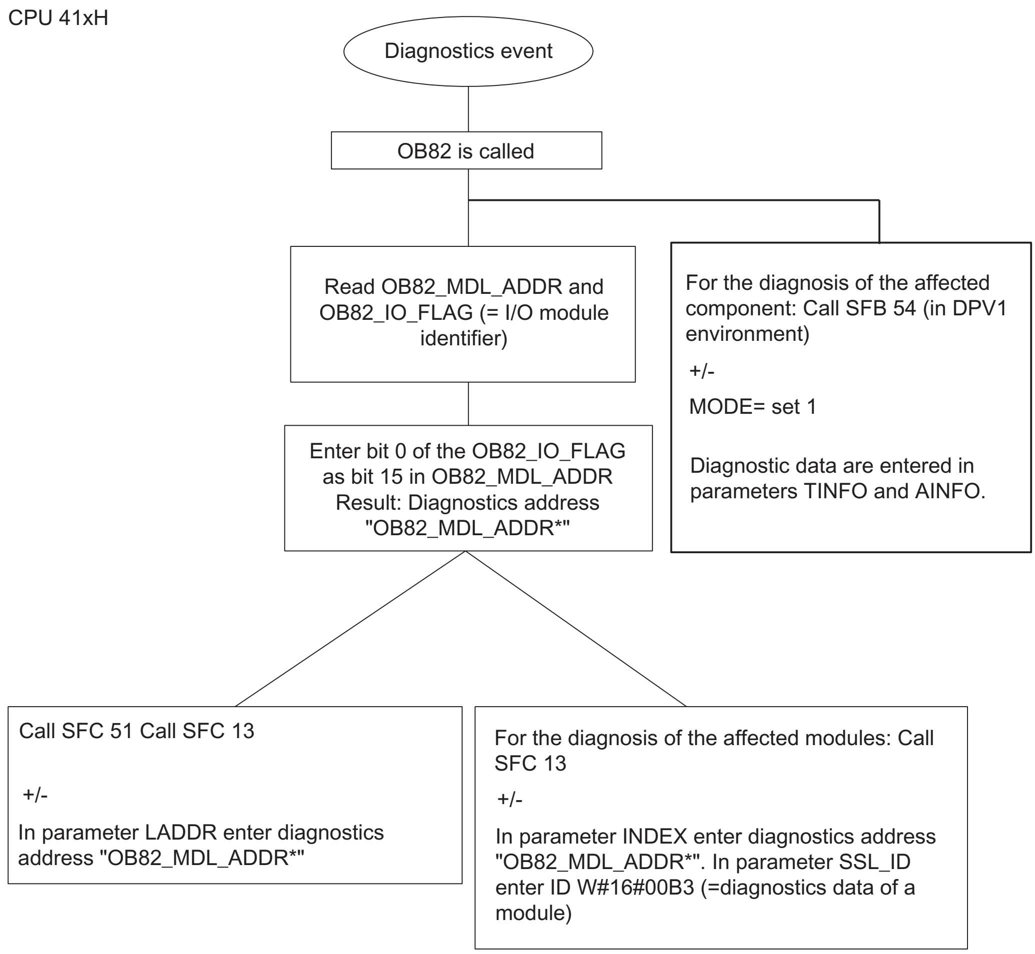


Figure 7-1 Diagnostics with CPU 41xH

Diagnostic addresses in connection with DP slave functionality

Assign the diagnostics addresses for PROFIBUS DP at the 41xH CPU. Verify in your configuration that the DP diagnostic addresses are assigned once to the DP master and once to the DP slave.

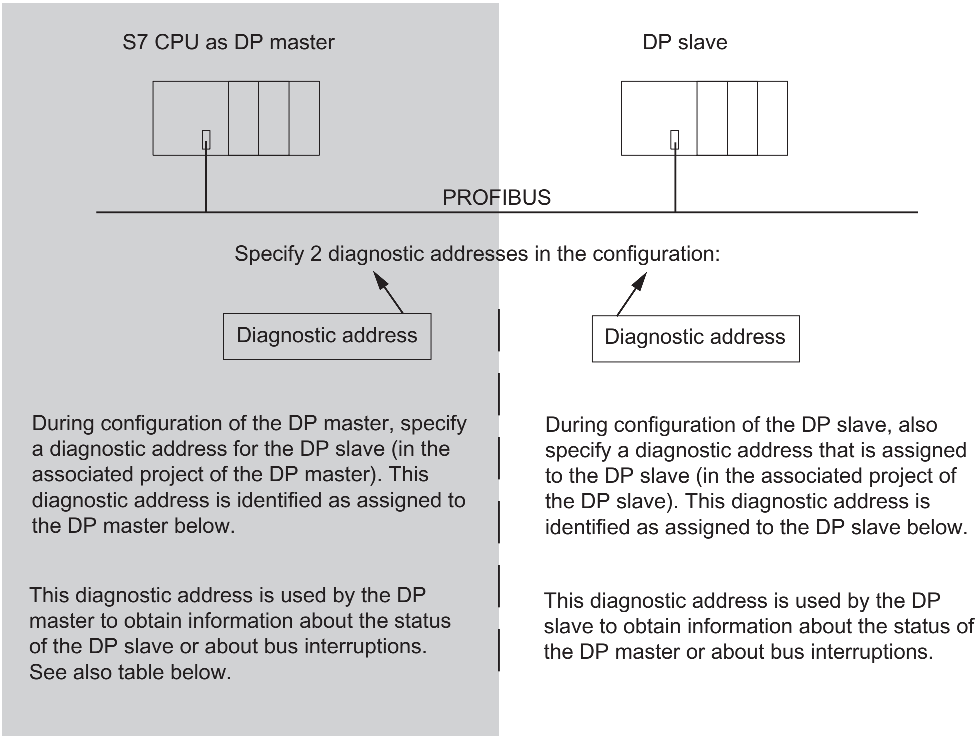


Figure 7-2 Diagnostic addresses for DP master and DP slave

Event detection

The following table shows how the CPU 41xH in DP master mode detects operating state changes on a DP slave or interruptions of the data transfer.

Table 7-4 Event detection of the CPU 41xH as a DP master

Event	What happens on the DP master
Bus interruption due to short-circuit or disconnection of the bus connector	• OB 86 is called with the message **Station failure** as an event entering state; diagnostic address of the DP slave assigned to the DP master • With I/O access: OB 122 called, I/O access error
DP slave: RUN → STOP	• OB 82 is called with the message **Module error** as event entering state; diagnostic address of the DP slave assigned to the DP master; variable OB82_MDL_STOP=1
DP slave: STOP → RUN	• OB is 82 called with the message **Module OK** as event exiting state; diagnostic address of the DP slave assigned to the DP master; variable OB82_MDL_STOP=0

Evaluation in the user program

The table below shows you how to evaluate RUN-STOP changes of the DP slave on the DP master. See previous table.

On the DP master	On the DP slave (CPU 41x)
• Example of diagnostic addresses: Master diagnostic address=1023 Slave diagnostic address on master system=1022	• Example of diagnostic addresses: Slave diagnostic address=422 Master diagnostic address = irrelevant
The CPU calls OB82 with at least the following information: • OB82_MDL_ADDR:=1022 • OB82_EV_CLASS:=B#16#39 As event entering state • OB82_MDL_DEFECT:=module fault The CPU diagnostic buffer also contains this information Your user program should also be set up to read the diagnostic data of the DP slave using SFC 13 "DPNRM_DG". Use SFB 54 in the DPV1 environment. This outputs the full interrupt information.	CPU: RUN → STOP CPU generates a DP slave diagnostic frame.

7.2 Consistent Data

Data that belongs together in terms of its content and a process state written at a specific point in time is known as consistent data. In order to maintain data consistency, do not modify or update the data during their transfer.

Example 1:

In order to provide a consistent image of the process signals to the CPU for the duration of cyclic program execution, the process signals are written to the process image of inputs prior to program execution, or the processing results are written to the process image of outputs after program execution. Subsequently, during program scanning when the inputs (I) and outputs (O) operand areas are addressed, the user program addresses the internal memory area of the CPU on which the image of the inputs and outputs is located instead of directly accessing the signal modules.

Example 2:

Inconsistency may develop when a communication block, such as SFB 14 "GET" or SFB 15 "PUT", is interrupted by a process alarm OB of higher priority. When the user program modifies any data of this process alarm OB which have already been processed by the communication block, certain parts of the transferred data will have retained their original status which was valid prior to process alarm processing, while others represent data from after process alarm processing.

This results in inconsistent data, i.e. data which are no longer associated.

SFC 81 "UBLKMOV"

Use SFC 81 ”UBLKMOV” to copy the content of a memory area of the source consistently to another memory area, namely the destination area. The copy operation can not be interrupted by other operating system activities.

SFC 81 "UBLKMOV" enables you to copy the following memory areas:

- Memory markers
- DB contents
- Process image of the inputs
- Process image of the outputs

The maximum amount of data you can copy is 512 bytes. Make allowances for the CPU-specific restrictions listed in the operation list.

Since copying can not be interrupted, the interrupt reaction times of your CPU may increase when using SFC 81 "UBLKMOV".

The source and destination areas must not overlap. If the specified destination area is larger than the source area, the function only copies as much data to the destination area as that contained in the source area. If the specified destination area is smaller than the source area, the function only copies as much data as can be written to the destination area.

7.2.1 Consistency of communication blocks and functions

Using S7-400 the communication data is not processed in the scan cycle checkpoint; instead, this data is processed in fixed time slices during the program cycle.

The system can always process the data formats byte, word and dword consistently, i.e. the transfer or processing of 1 byte, 1 word = 2 bytes or 1 dword = 4 bytes can not be interrupted.

When the user program calls communication blocks such as SFB 12 BSEND" and SFB 13 BRCV", which are only used in pairs and access shared data, the access to this data area can be coordinated by means of the actual "DONE" parameter, for example. Data consistency of the communication areas transmitted locally with a communication block can thus be ensured in the user program.

In contrast, S7 communication functions do not require a block, such as SFB 14 ”GET”, SFB 15 ”PUT”, in the user program of the PLC. Here, you must make allowance for the volume of consistent data in the programming phase.

7.2.2 Access to the CPU RAM

The communication functions of the operating system access the CPU RAM in fixed block lengths. The block length is CPU-specific. The tags for S7-400 CPUs have a length of up to 472 bytes.

This ensures that the interrupt reaction time is prolonged not due to communication load. Since this access is performed asynchronously to the user program, you can not transmit an unlimited number of bytes of consistent data.

The rules to ensure data consistency are described below.

7.2.3 Consistency rules for SFB 14 "GET" or reading tag and SFB 15 "PUT" or writing tag

SFB 14

The data are received consistently if you observe the following points:

Evaluate the entire, currently used part of the receive area RD_i before you activate a new request.

SFB 15

When you initiate a send operation (positive edge at REQ), the system copies the data of the send data areas SD_i to be transferred from the user program. You can write new data to these areas after the block call, without any risk of corrupting the current send data.

Note

Completion of transfer

The transfer operation is not completed until the status parameter DONE assumes the value 1.

7.2.4 Reading data consistently from a DP standard slave and writing consistently to a DP standard slave

Reading data consistently from a DP standard slave using SFC 14 "DPRD_DAT"

Use SFC 14 "DPRD_DAT", "read consistent data of a DP standard slave", to read consistent data from a DP standard slave.

The data read is entered into the destination range defined by RECORD if no error occurs during the data transmission.

The destination range must have the same length as the one you have configured for the selected module with STEP 7.

By calling SFC 14 you can only access the data of one module / DP ID at the configured start address.

Writing data consistently to a DP standard slave using SFC 15 "DPWR_DAT"

Use SFC 15 "DPWR_DAT", "write consistent data to a DP standard slave", to transfer consistent data in RECORD to the addressed DP standard slave.

The source area must be the same length as the one you have configured for the selected module with STEP 7.

Upper limit for the transfer of consistent user data to a DP slave

The PROFIBUS DP standard defines upper limits for the transfer of consistent user data to a DP slave.

For this reason a maximum of 64 words = 128 bytes of user data can be consistently transferred in a block to the DP slave.

You can define the length of consistent area in your configuration. In the special identification format (SIF), you can define a maximum length of consistent data of 64 words = 128 bytes, 128 bytes for inputs, and 128 bytes for outputs. Any greater length value is not possible.

This upper limit applies only to pure user data. Diagnostics and parameter data will be grouped to form complete data records, and are thus always transferred consistently.

In the general identification format (GIF), you can define a maximum length of consistent data of 16 words = 32 bytes, 32 bytes for inputs, and 32 bytes for outputs. Any greater length value is not possible.

In this context, make allowances for the fact that a 41x CPU operating as DP slave generally has to support its configuration at an external master (implementation by means of GSD file) using the general identification format. A 41x CPU operated as DP slave thus supports only a maximum length of 16 words = 32 bytes in its transfer memory for PROFIBUS DP.

7.2.5 Consistent data access without using SFC 14 or SFC 15

Consistent data access > 4 bytes is also possible without using SFC14 or SFC15. The data area of a DP slave which is to be transferred consistently will be written to a process image partition. The data in this area are thus always consistent. You can then access the process image partition using the load / transfer commands (L EW 1, for example). This represents a highly user-friendly and efficient (low runtime load) method to access consistent data and to implement and configure such devices as drives or other DP slaves.

Any direct access to a data area which is configured consistent,
such as L PEW or T PAW, does **not** result in an I/O access error.

Important aspects in the conversion from the SFC14/15 solution to the process image solution are:

- When converting from the SFC14/15 method to the process image method, it is not advisable to use the system functions and the process image at the same time. Although the process image is updated when writing with the system function SFC15, this is not the case when reading. In other words, consistency between the values of the process image and of the system function SFC14 is not ensured.
- SFC 50 "RD_LGADR" outputs another address area with the SFC 14/15 method as with the process image method.
- When using a CP 443-5 ext, the parallel use of system functions and of the process image leads to the following errors : Read/write access to the process image is blocked, and/or SFC 14/15 is no longer able to perform any read/write access operations .

Example:

The example of the process image partition 3 "TPA 3" below shows a possible configuration in HW Config:

- TPA 3 at output: Those 50 bytes are stored consistently in process image partition 3 (pulldown list "Consistent over > entire length"), and can thus be read by means of standard "Load input xy" commands.
- Selecting "Process Image Partition -> ---" under Input in the pulldown menu means: do not write data to the process image. You must work with the system functions SFC14/15.

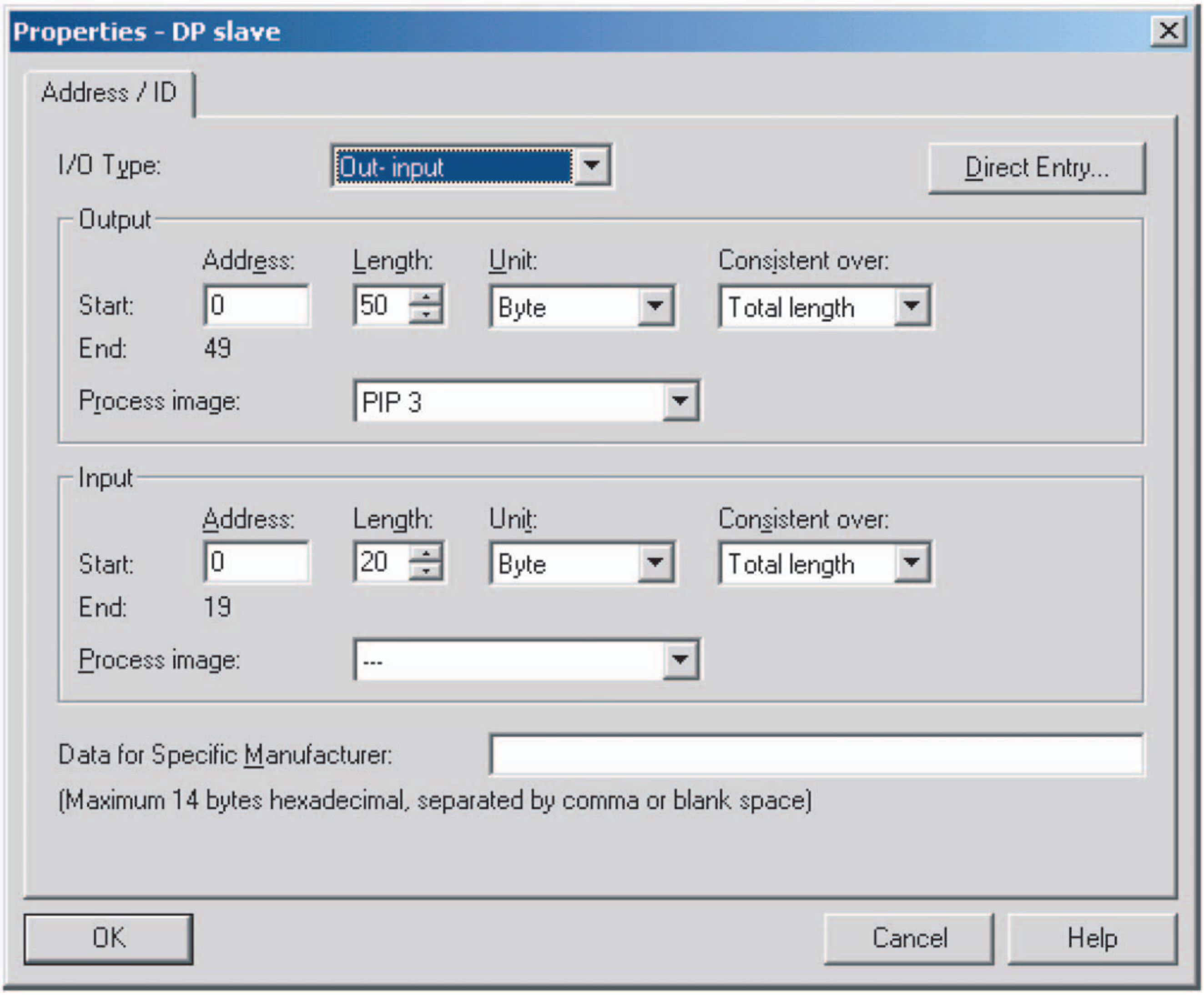


Figure 7-3 DP slave properties

System and operating states of the S7–400H 8

8.1 System and operating states of the S7–400H

This chapter features an introduction to the subject of S7-400H fault-tolerant systems.

You will learn the basic concepts that are used in describing how fault-tolerant systems operate.

Following that, you will receive information on fault-tolerant system modes. These modes depend on the operating states of the different fault-tolerant CPUs, which will be described in the section that follows after that one.

In describing these operating states, this section concentrates on the behavior that differs from a standard CPU. You will find a description of the normal behavior of a CPU in the corresponding operating state in the *Programming with STEP 7* manual.

The final section provides details on the modified time response of fault-tolerant CPUs.

8.2 Introduction

The S7-400H consists of two redundant configured subsystems that are synchronized via fiber-optic cables.

The two subsystems create a redundant automation system operating with a two-channel (1-of-2) structure based on the "active redundancy" principle.

What does active redundancy mean?

Active redundancy, commonly also referred to as functional redundancy, means that all redundant resources are constantly in operation and simultaneously involved in the execution of the control task.

For the S7-400H this means that the user programs in both CPUs are identical and executed synchronously by the CPUs.

Conventions

To distinguish between the two units, we use the traditional expressions of "master" and "standby" for dual-channel fault-tolerant systems in this description. The standby always processes events in synchronism with the master, and does not explicitly wait for any errors before doing so.

The distinction made between the master and standby CPUs is primarily important for ensuring reproducible error reactions. So the standby CPU may go into STOP when the redundant link fails, while the master CPU remains in RUN.

Master/standby assignment

When the S7-400H is initially switched on, the first CPU to be started assumes master mode, and the partner CPU assumes standby mode.

The preset master/standby assignment is retained when both CPUs simultaneously POWER ON.

The master/standby setting changes when:

1. the standby CPU starts up before the master CPU (interval of at least 3 s)
2. the redundant master CPU fails or goes into STOP
3. No error was found in TROUBLESHOOTING mode (see also section TROUBLESHOOTING operating state (Page 92))

Synchronizing the subsystems

The master and standby CPUs are linked by fiber-optic cables. The redundant CPUs maintain event-driven synchronous program execution via this coupling.

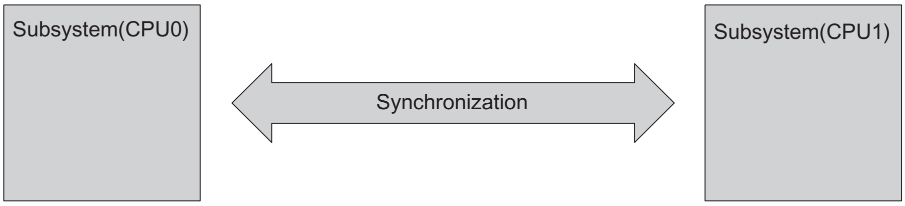


Figure 8-1 Synchronizing the subsystems

Synchronization is performed automatically by the operating system and has no effect on the user program. You create your program in the same way as for standard S7-400 CPUs.

Event-driven synchronization

The "event-driven synchronization" procedure patented by Siemens was used for the S7-400H. This procedure has proved itself in practice and has already been used for the S5-115H and S5-155H controllers.

Event-driven synchronization means that the master and standby always synchronize their data when an event occurs which may lead to different internal states of the subsystems.

The master and standby CPUs are synchronized when:

- There is direct access to the I/O
- Interrupts occur
- User timers - for example, S7 timers are updated
- Data is modified by communication functions

Continued bumpless operation if CPU redundancy is lost

The event-driven synchronization method ensures bumpless continuation of operation by the standby CPU even if the master CPU fails.

Self-test

Malfunctions or errors must be detected, localized and reported as quickly as possible. Consequently, extensive self-test functions have been implemented in the S7-400H that run automatically and entirely in the background.

The following components and functions are tested:

- Linking of the central modules
- Processor
- Internal memory of the CPU
- I/O bus

If the self-test detects an error, the fault-tolerant system tries to eliminate it or to suppress its effects.

For detailed information on the self-test, refer to section Self-test (Page 94).

8.3 The system states of the S7-400H

The system states of the S7-400H derive from the operating states of the two CPUs. The term "system state" is used as a simplified term which identifies the concurrent operating states of the two CPUs.

Example: Instead of "the master CPU is in RUN and the standby CPU is in LINK-UP mode" we say "the S7-400H system is in link-up mode".

Overview of system states

The table below provides an overview of the various possible states of the S7-400H system.

Table 8-1 Overview of S7-400H system states

System states of the S7–400H	Operating states of the two CPUs	
	Master	Standby
Stop	STOP	STOP, power off, DEFECTIVE
Startup	STARTUP	STOP, power off, DEFECTIVE, no synchronization
Single mode	RUN	STOP, TROUBLESHOOTING, power off, DEFECTIVE, no synchronization
Link-up	RUN	STARTUP, LINK-UP
Update	RUN	UPDATE
Redundant	RUN	RUN
Hold	HOLD	STOP, TROUBLESHOOTING, power off, DEFECTIVE, no synchronization

8.4 The operating states of the CPUs

Operating states describe the behavior of the CPUs at any given point in time. Knowledge of the operating states of the CPUs is useful for programming startup, the test, and the error diagnostics.

Operating states from POWER ON to system redundancy

Generally speaking, the two CPUs enjoy equal rights so that either can be the master or the standby CPU. For reasons of legibility, the illustration presumes that the master CPU (CPU 0) is started up before the standby CPU (CPU 1) is switched on.

The following figure shows the operating states of the two CPUs, from POWER ON to system redundancy mode. The HOLD HOLD operating state (Page 92) and TROUBLESHOOTING TROUBLESHOOTING operating state (Page 92) modes are special modes and are not shown.

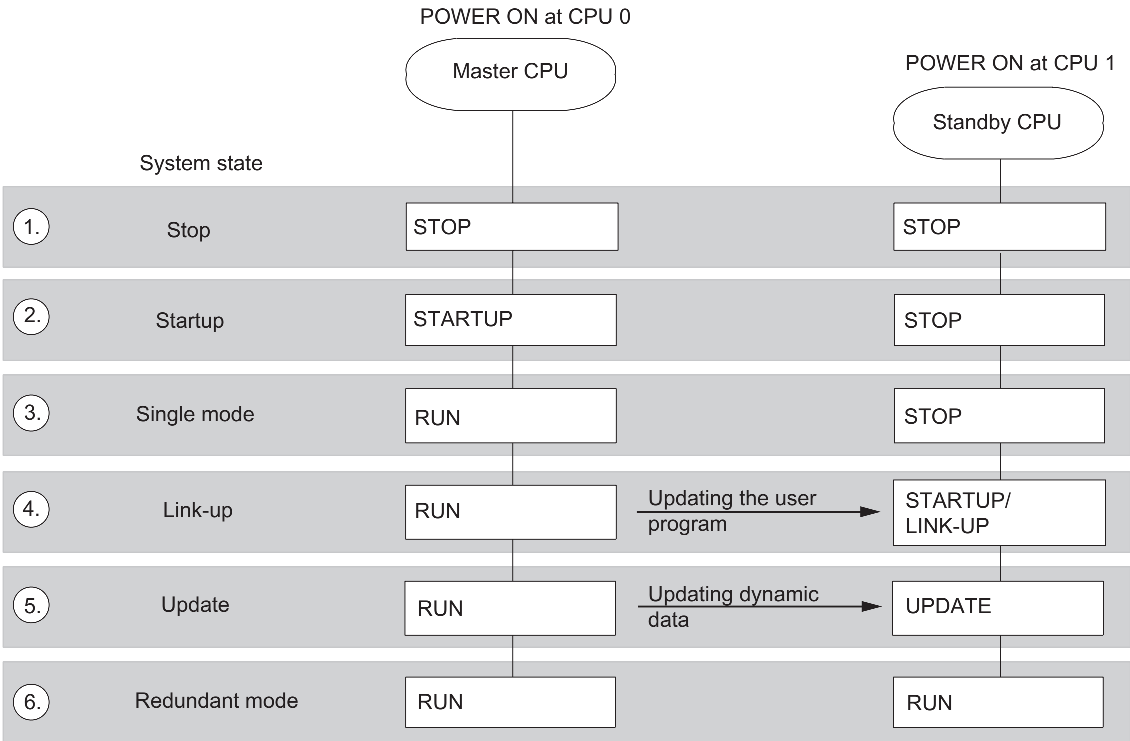


Figure 8-2 System and operating modes of the fault-tolerant system

Explanation of the diagram

Point	Description
1.	After the power supply has been turned on, the two CPUs (CPU 0 and CPU 1) are in STOP mode.
2.	CPU 0 changes to STARTUP and executes OB 100 or OB 102 according to the startup mode; see also section STARTUP operating state (Page 90).
3.	If startup is successful, the master CPU (CPU 0) changes to single mode. The master CPU executes the user program alone. At the transition to the LINK-UP system state, no block may be opened by the "Monitor" option, and no variable table may be active.
4.	If the standby CPU (CPU 1) requests LINK-UP, the master and standby CPUs compare their user programs. If any differences are found, the master CPU updates the user program of the standby CPU; see also section LINK-UP and UPDATE operating states (Page 90).
5.	After a successful link-up, updating is started, see section Update sequence (Page 107). The master CPU updates the dynamic data of the standby CPU. Dynamic data means inputs, outputs, timers, counters, bit memory and data blocks. Following the update, the memory of both CPUs has the same content; see also section LINK-UP and UPDATE operating states (Page 90).
6.	The master and standby CPUs are in RUN after the update. Both CPUs process the user program synchronized with each other. Exception: Master/standby changeover for configuration/program modifications. The redundant mode is only supported when both CPUs are the same version and have the same firmware version.

8.4.1 STOP operating state

Except for the additions described below, the behavior of S7-400H CPUs in STOP corresponds to that of standard S7-400 CPUs.

When you download a configuration to one of the CPUs while both are in STOP, observe the points below:

- Start the CPU to which you downloaded the configuration first, in order to set it up for master mode.
- By initiating the system startup request on the programming device, you first start the CPU to which an online connection exists, regardless of the master or standby status.

NOTICE
A system startup may trigger a master-standby changeover.

Memory reset

The memory reset function affects only the selected CPU. To reset both CPUs, you must reset one and then the other.

8.4.2 STARTUP operating state

Except for the additions described below, the behavior of S7-400H CPUs in STARTUP corresponds to that of standard S7-400 CPUs.

Startup modes

The fault-tolerant CPUs distinguish between cold start and warm restart.

Fault-tolerant CPUs do not support hot restarts.

Startup processing by the master CPU

The startup system state of an S7-400H is always processed by the master CPU.

During STARTUP, the master CPU compares the existing I/O configuration with the hardware configuration that you created in STEP 7. If any differences are found, the master CPU reacts in the same way as a standard S7-400 CPU.

The master CPU checks and configures:

- the switched I/O
- its assigned one-sided I/O

Startup of the standby CPU

The standby CPU startup routine does not call an OB 100 or OB 102.

The standby CPU checks and configures:

- its assigned one-sided I/O

Further information

For detailed information on STARTUP states, refer to the *Programming with STEP 7* manual.

8.4.3 LINK-UP and UPDATE operating states

The master CPU checks and updates the memory content of the standby CPU before the fault-tolerant system assumes redundant mode. This action involves two successive phases, termed link-up and update.

The master CPU is always in RUN and the standby CPU is in LINK-UP or UPDATE status during the link-up and update phases.

In addition to the link-up and update functions which are carried out in order to establish system redundancy, the system also supports linking and updating in combination with master/standby changeover.

For detailed information on link-up and updating, refer to section Link-up and update (Page 99).

8.4.4 RUN operating state

Except for the additions described below, the behavior of S7-400H CPUs in RUN corresponds to that of standard S7-400 CPUs.

The user program is executed by at least one of the two CPUs in the following system states:

- Single mode
- Link-up, Update
- Redundant

Single mode, Link-up, Update

In the system states mentioned above, the master CPU is in RUN and executes the user program in single mode.

Redundant mode

The master and standby CPUs are always in RUN when operating in redundant state, execute the user program in synchronism, and perform mutual checks.

In the redundant state it is not possible to test the user program with breakpoints.

The redundant state is only supported with CPUs of the same version and firmware version. Redundancy will be lost if one of the errors listed in the following table occurs.

Table 8-2 Causes of error leading to redundancy loss

Cause of error	Reaction
Failure of one CPU	Failure and replacement of a CPU (Page 202)
Failure of the redundant link (synchronization module or fiber-optic cable)	Failure and replacement of a synchronization module or fiber-optic cable (Page 208)
RAM comparison error	TROUBLESHOOTING operating state (Page 92)

Redundant use of modules

The following rule applies to the redundant state:

Modules interconnected in redundant mode, such as DP slave interface module IM 153-2, must be in identical pairs, i.e. the two redundant linked modules have the same order number, release and firmware version.

8.4.5 HOLD operating state

Except for the additions described below, the behavior of the S7-400H CPU in HOLD corresponds to that of a standard S7-400 CPU.

The HOLD state has an exceptional role, as it is used only for test purposes.

When is the HOLD operating state possible?

A transition to HOLD is only available during STARTUP and in RUN in single mode.

Properties

- Link-up and update operations are not available while the fault-tolerant CPU is in HOLD; the standby CPU remains in STOP and outputs a diagnostics message.
- It is not possible to set breakpoints if the fault-tolerant system remains in the redundant state.

8.4.6 TROUBLESHOOTING operating state

The TROUBLESHOOTING mode can only be adopted from the Redundant mode. During troubleshooting, the CPUs exit the redundant mode, the other CPU becomes master and continues to work in single mode.

Note

If the master CPU changes to STOP during troubleshooting, the troubleshooting is continued on the standby CPU. However, when troubleshooting is completed, the standby CPU does not start up again.

The self-test routine compares the master and standby CPUs, and reports an error if any differences are found. Errors could be caused by hardware faults, checksum errors and RAM/PIO comparison errors.

The following events will trigger the TROUBLESHOOTING state:

1. If a one-sided call of OB 121 (on only one CPU) occurs in redundant mode, the CPU assumes a hardware fault and enters the TROUBLESHOOTING state. The partner CPU assumes master mode as required, and continues operation in single mode.
2. When a checksum error occurs on only one of the redundant CPUs, that CPU enters the TROUBLESHOOTING state. The partner CPU assumes master mode as required, and continues operation in single mode.
3. When a RAM/PIO comparison error is detected in redundant mode, the standby CPU enters the TROUBLESHOOTING state (default reaction), and the master CPU continues operation in single mode.

   The reaction to RAM/PIO comparison errors can be modified in the configuration (for example, the standby CPU goes into STOP).

4. When a multiple-bit error occurs on only one of the redundant CPUs, that CPU will enter the TROUBLESHOOTING state. The partner CPU assumes master mode as required, and continues operation in single mode.

   But: OB 84 is called when a single-bit error occurs on one of the redundant CPUs. The CPU does not change to TROUBLESHOOTING mode.

5. If synchronization is lost during redundant mode, the standby CPU changes to TROUBLESHOOTING mode. The other CPU remains master and continues operation in single mode.

The TROUBLESHOOTING MODE is set to allow a faulty CPU to be localized. The standby CPU runs the full self-test, while the master CPU remains in RUN.

If a hardware fault is detected, the CPU changes to DEFECTIVE mode. If no fault is detected the CPU is linked up again. The fault-tolerant system resumes the redundant system state. An automatic master-standby changeover then takes place. This ensures that when the next error is detected in troubleshooting mode, the hardware of the previous master CPU is tested.

No communication is possible with the CPU in TROUBLESHOOTING mode, for example no access by a programming device. The TROUBLESHOOTING mode is indicated by the RUN and STOP LEDs; see section Status and error displays (Page 46).

For further information on the self-test, refer to section Self-test (Page 94)

8.5 Self-test

Processing the self-test

The CPU executes the complete self-test program after POWER ON without backup, such as POWER ON after initial insertion of the CPU or POWER ON with no backup battery, and in the TROUBLESHOOTING state. The self-test takes about 10 minutes.

When the CPU of a fault-tolerant system request a memory reset and is then shut down with backup power, it performs a self-test irrespective of the backup function. The CPU requests a memory reset when you remove the memory card, for example.

In RUN the operating system splits the self-test routine into several small program sections, so-called test slices, which are processed in multiple successive cycles. The cyclic self-test is organized to perform a single, complete pass in a certain time. The default time of 90 minutes can be modified in the configuration.

Reaction to errors during the self-test

If the self-test returns an error, the following happens:

Table 8-3 Reaction to errors during the self-test

Error class	System reaction
Hardware fault without one-sided call of OB 121	The faulty CPU enters the DEFECTIVE state. The fault-tolerant system switches to single mode. The cause of the error is written to the diagnostics buffer.
Hardware fault with one-sided call of OB 121	The CPU with the one-sided OB 121 enters the TROUBLESHOOTING state. The fault-tolerant system switches to single mode (see below).
RAM/PIO comparison error	The cause of the error is written to the diagnostics buffer. The CPU enters the configured system or operating state (see below).
Checksum errors	The reaction depends on the error situation (see below).
Multiple-bit errors	The faulty CPU enters the TROUBLESHOOTING state.

Hardware fault with one-sided call of OB 121

If a hardware fault occurs with a one-sided OB121 call for the first time since the previous POWER ON without backup, the faulty CPU enters the TROUBLESHOOTING state. The fault-tolerant system switches to single mode. The cause of the error is written to the diagnostics buffer.

RAM/PIO comparison error

If the self-test returns a RAM/PIO comparison error, the fault-tolerant system quits redundant mode and the standby CPU enters the TROUBLESHOOTING state (in default configuration). The cause of the error is written to the diagnostics buffer.

The reaction to a recurring RAM/PIO comparison error depends on whether the error occurs in the subsequent self-test cycle after troubleshooting or not until later.

Table 8-4 Reaction to a recurring comparison error

Comparison error recurs ...	Reaction
in the first self-test cycle after troubleshooting	The standby CPU first enters the TROUBLESHOOTING state, and then goes into STOP. The fault-tolerant system switches to single mode.
after two or more self-test cycles after troubleshooting	Standby CPU enters the TROUBLESHOOTING state. The fault-tolerant system switches to single mode.

Checksum errors

When a checksum error occurs for the first time after the last POWER ON without backup, the system reacts as follows:

Table 8-5 Reaction to checksum errors

Time of detection	System reaction
During the startup test after POWER ON	The faulty CPU enters the DEFECTIVE state. The fault-tolerant system switches to single mode.
In the cyclic self-test (STOP or single mode)	The error is corrected. The CPU remains in STOP or in single mode.
In the cyclic self-test (redundant system state)	The error is corrected. The faulty CPU enters the TROUBLESHOOTING state. The fault-tolerant system switches to single mode.
In the TROUBLESHOOTING state	The faulty CPU enters the DEFECTIVE state.
Single-bit errors	The CPU calls OB 84 after the detection and elimination of the error.

The cause of the error is written to the diagnostics buffer.

In an F system, the F program is informed that the self-test has detected an error the first time a checksum error occurs in STOP or single mode. The reaction of the F program to this is described in the *S7-400F and S7-400FH Automation Systems* manual.

Hardware fault with one-sided call of OB 121, checksum error, second occurrence

A 41x-4H CPU reacts to a second occurrence of a hardware fault with a one-sided call of OB 121 and to checksum errors as set out in the table below, based on the various operating modes of the 41x-4H CPU.

Table 8-6 Hardware fault with one-sided call of OB 121, checksum error, second occurrence

Error	CPU in single mode	CPU in stand-alone mode	CPU in redundant mode
Hardware fault with one-sided call of OB 121	OB 121 is executed	OB 121 is executed	The faulty CPU enters the TROUBLESHOOTING state. The fault-tolerant system switches to single mode.
Checksum errors	The CPU enters the DEFECTIVE state if two errors occur within two successive test cycles. (Configure the length of the test cycle in HW Config)	The CPU enters the DEFECTIVE state if two errors occur within two successive test cycles. (Configure the length of the test cycle in HW Config)	The CPU enters the DEFECTIVE state if a second error triggered by the first error event occurs within the troubleshooting state.

If a second checksum error occurs in single/stand-alone mode after twice the test cycle time has expired, the CPU reacts as it did on the first occurrence of the error. If a second error (hardware fault with one-sided call of OB 121, checksum error) occurs in redundant mode when troubleshooting is finished, the CPU reacts as it did on the first occurrence of the error.

Multiple-bit errors

The CPU changes to TROUBLESHOOTING mode when a multiple-bit error is detected while the fault-tolerant system is operating in redundant mode. When troubleshooting is finished, the CPU can automatically link and update itself, and resume redundant operation. At the transition to troubleshooting mode, the address of the triggering error is reported in the diagnostics buffer.

Single-bit errors

The CPU calls OB 84 after the detection and elimination of the error.

Influencing the cyclic self-test

SFC90 "H_CTRL" allows you to influence the scope and execution of the cyclic self-test. For example, you can remove various test components from the overall test and re-introduce them. In addition, you can explicitly call specific test components and then initiate processing of them.

For detailed information on SFC90 "H_CTRL", refer to the *System Software for S7-300/400, System and Standard Functions* manual.

NOTICE
In a fail-safe system, you are not allowed to disable and then re-enable the cyclic self-tests. For more details, refer to the *S7-400F and S7-400FH Programmable Controllers* manual.

8.6 Time-based reaction

Instruction run times

You will find the execution times of the STEP 7 instructions in the operation list for the S7-400 CPUs.

Processing I/O direct access

Please note that any I/O access always requires a synchronization of the two units, and so extends the cycle time.

You should therefore avoid any direct I/O access in your user program, and instead access the data using the process images (or the process image partitions, for example when handling cyclic interrupts). This automatically increases performance, because in process images you can always synchronize a whole set of values at once.

Reaction time

For detailed information on calculating reaction times, refer to section S7-400 cycle and reaction times (Page 291).

Note that any update of the standby CPU extends the interrupt reaction time.

The interrupt reaction time depends on the priority class, because a graduated delay of the interrupts is performed during an update.

8.7 Evaluation of process interrupts in the S7-400H system

When using a process interrupt-triggering module in the S7-400H system, it is possible that the process values which can be read from the process interrupt OB by direct access do not match the process values valid at the time of the interrupt. Evaluate the temporary tags (start information) in the process interrupt OB instead.

So when using the process alarm-triggering module SM 321-7BH00 it is not advisable to have different reactions to positive or negative edges at the same input, because this would require direct access to the I/O. If you want to react differently to the two edge transitions in your user program, assign the signal to two inputs from different channel groups and configure one input for the positive edge and the other for the negative edge.

9 Link-up and update

9.1 Effects of link-up and updating

Link-up and updating are indicated by the REDF LEDs on the two CPUs. During link-up, the LEDs flash at a frequency of 0.5 Hz, and when updating at a frequency of 2 Hz.

Link-up and update have various effects on user program execution and on communication functions.

Table 9-1 Properties of link-up and update functions

Process	Link-up	Update
Execution of the user program	All priority classes (OBs) are processed.	Processing of the priority classes is delayed section by section. All the requirements are caught up with after the update. For details, refer to the sections below.
Deletion, loading, generating and compressing blocks	Blocks can not be deleted, loaded, created or compressed. When such actions are busy, link-up and updating are inhibited.	Blocks can not be deleted, loaded, created or compressed.
Execution of communication functions, PG operation	Communication functions are executed.	Execution of the functions is restricted section by section and delayed. All the delayed functions are caught up with after the update. For details, refer to the sections below.
CPU self-test	Not performed	Not performed
Test and commissioning functions, such as "Monitor and Control Tag", "Monitor (On/Off)"	Test and commissioning functions are disabled. When such actions are busy, link-up and update operations are inhibited.	Test and commissioning functions are disabled.
Handling of the connections to the master CPU	All connections are retained; no new connections can be made.	All connections are retained; no new connections can be made. Aborted connections are not restored until the update is completed
Handling of the connections to the standby CPU	All the connections are cancelled; no new connections can be made.	All connections are already down. They were cancelled during link-up.

9.2 Conditions for link-up and update

Which commands you can use on the PG to initiate a link-up and update operation is determined by the conditions on the master and standby CPU. The table below shows the correlation between those conditions and available PG commands for link-up and update operations.

Table 9-2 Conditions for link-up and update

Link-up and update as PG command:	Size and type of load memory in the master and standby CPUs	FW version in the master and standby CPUs	Available sync links	Hardware version on master and standby CPU
Restart of the standby	are identical	are identical	2	are identical
Switch to CPU with modified configuration	RAM and EPROM mixed	are identical	2	are identical
Switch to CPU with expanded memory configuration	Size of load memory in the standby CPU is larger than that of the master	are identical	2	are identical
Switch to CPU with modified operating system	are identical	are different	2	are identical
CPUs with changed hardware version	are identical	are identical	2	are different
Only one synchronization link-up is available over one intact redundant link	are identical	are identical	1	are identical

9.3 Link-up and update

There are two types of link-up and update operation:

- Within a "normal" link-up and update operation, the fault-tolerant system should change over from single mode to redundant mode. The two CPUs then process the same program synchronized with each other.
- When the CPUs link up and update with master/standby changeover, the second CPU with modified components can assume control over the process. Either the hardware configuration, or the memory configuration, or the operating system may have been modified.

  In order to return to the redundant state, a "normal" link-up and update operation must be performed subsequently.

How to start the link-up and update operation?

Initial situation: Single mode, i.e. only one of the CPUs of a fault-tolerant system connected via fiber-optic cables is in RUN.

To establish system redundancy, initiate the link-up and update operation as follows:

- Toggle the mode selector switch of the standby CPU from STOP to RUN.
- POWER ON the standby (mode selector switch in RUN position), if prior to POWER OFF the CPU was not in STOP mode.
- Operator input on the PG/ES.

A link-up and update operation with master/standby changeover is always started on the PG/ES.

NOTICE
If a link-up and update operation is interrupted on the standby CPU (for example due to POWER OFF, STOP), this may cause data inconsistency and lead to a memory reset request on this CPU. The link-up and update functions are possible again after a memory reset on the standby.

Flow chart of the link-up and update operation

The diagram below outlines the general sequence of the link-up and update. In the initial situation, the master is operating in single mode. In the figure, CPU 0 is assumed to be the master.

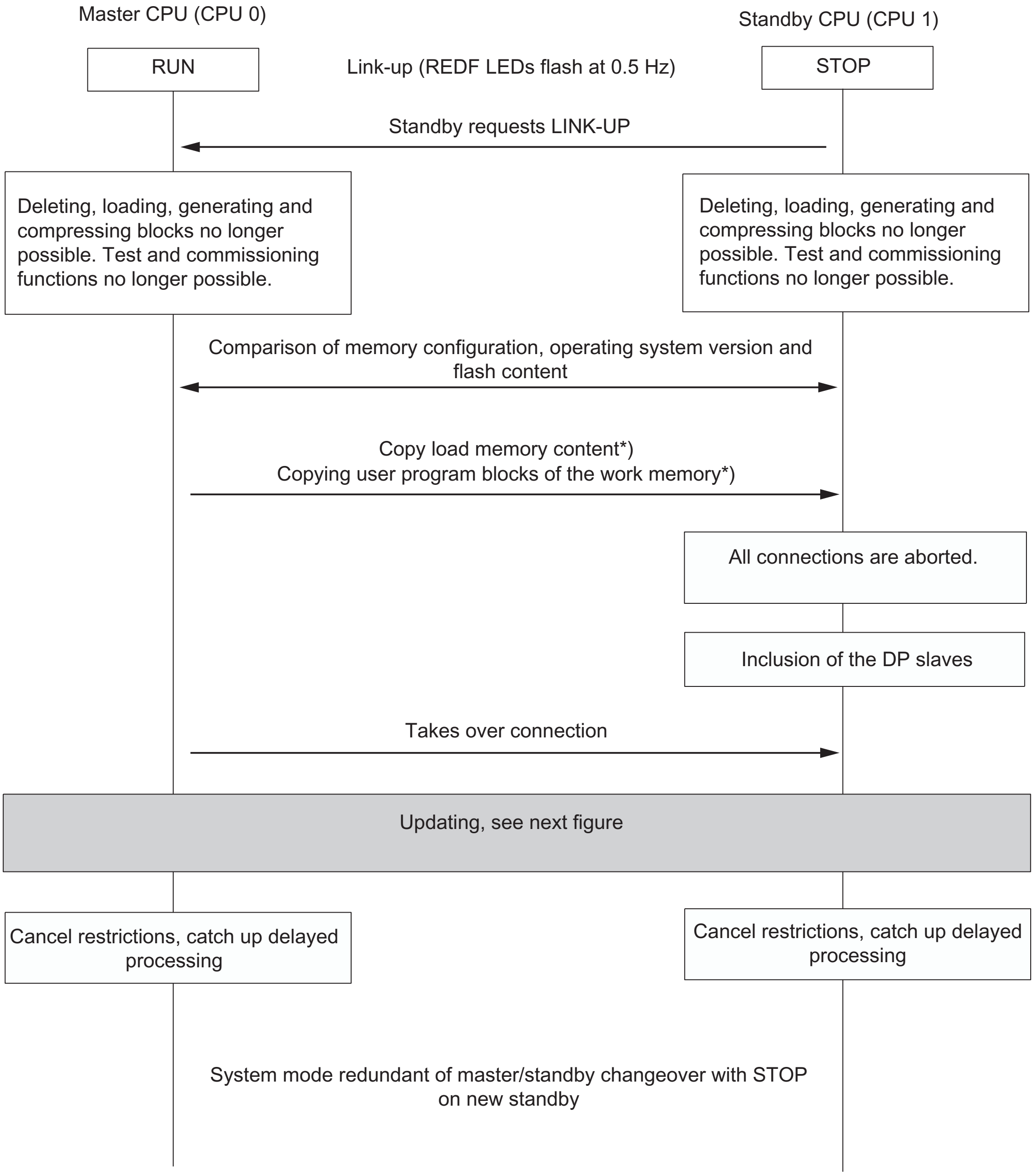


Figure 9-1 Sequence of link-up and update

*) If the "Switch to CPU with altered configuration" option is set, the content of the load memory is not copied; what is copied from the user program blocks of the work memory (OBs, FCs, FBs, DBs, SDBs) of the master CPU is listed in section Switch to CPU with modified configuration or expanded memory configuration (Page 110)

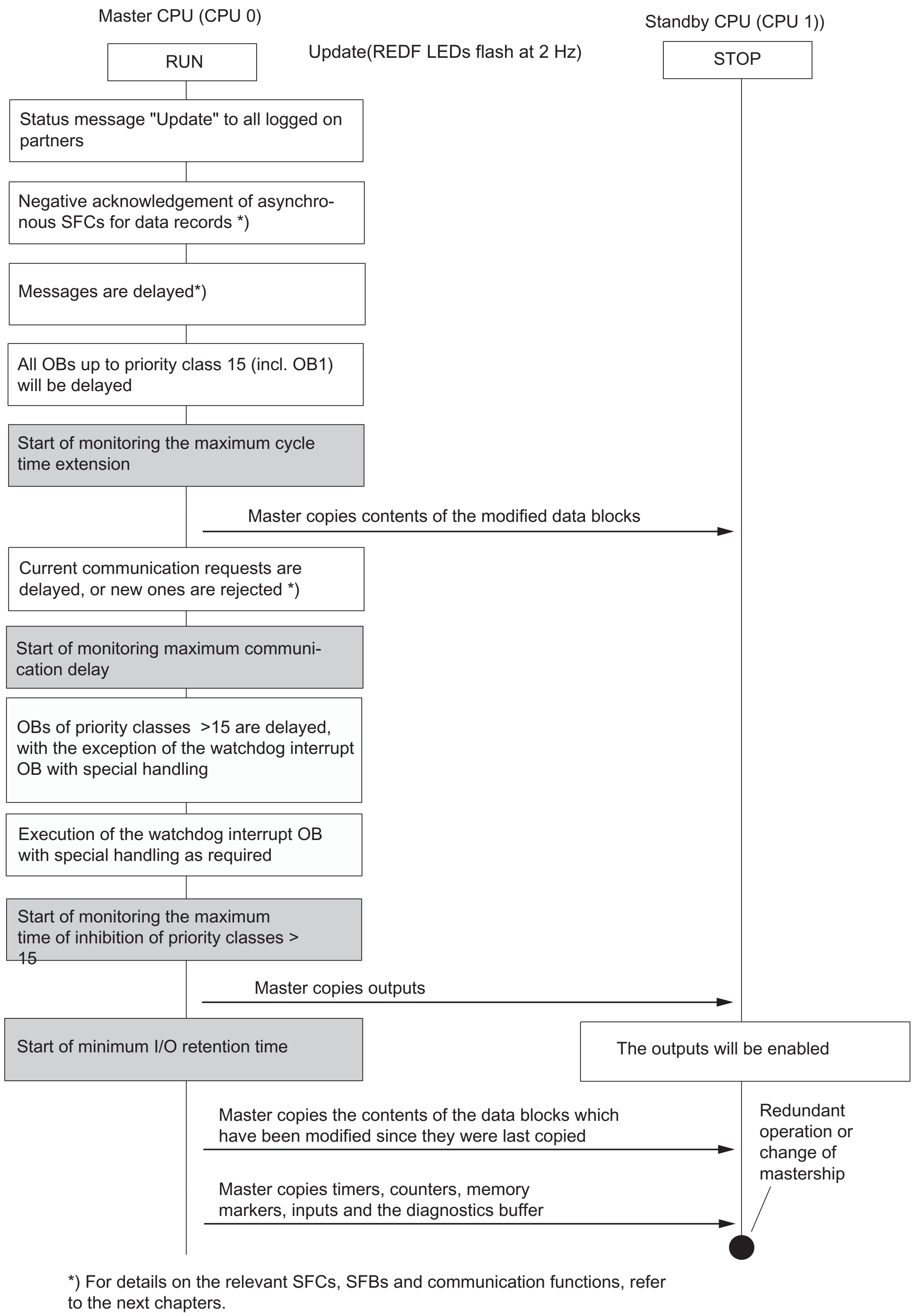


Figure 9-2 Update sequence

Minimum duration of input signals during update

Program execution is stopped for a certain time during the update (the sections below describe this in greater detail). To ensure that the CPU can reliably detect changes to input signals during the update, the following condition must be satisfied:

Min. signal duration > 2 x the time required for I/O update (DP only)
+ call interval of the priority class
+ program execution time of the priority class
+ time required for the update
+ program execution time of higher-priority classes

Example:

Minimum signal duration of an input signal that is evaluated in a priority class > 15 (for example, OB 40).

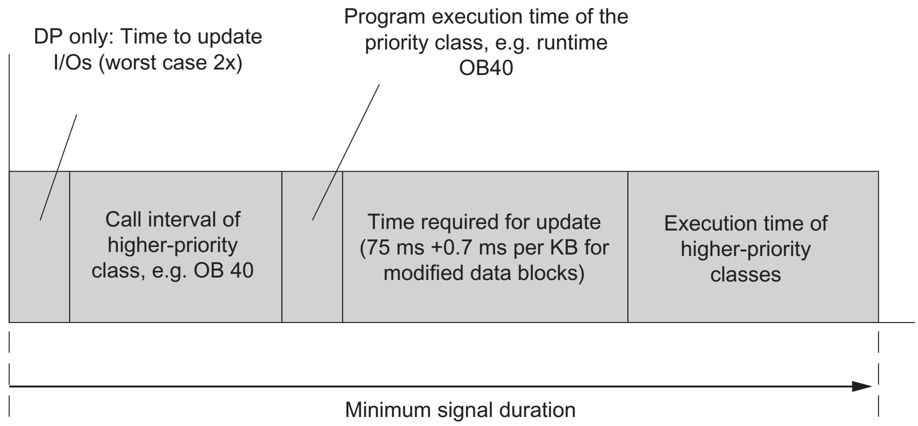


Figure 9-3 Example of minimum signal duration of an input signal during the update

9.3.1 Link-up sequence

For the link-up, you need to decide whether to carry out a master/standby changeover, or whether to conclude the operation by setting the system to redundant state.

Link-up with the objective of setting up system redundancy

To exclude differences in the two subsystems, the master and the standby CPU run comparisons.

The following are compared::

1. Consistency of the memory configuration
2. Consistency of the operating system version
3. Consistency of the load memory (FLASH card) content
4. Consistency of load memory (integrated RAM and RAM card) content

If 1, 2, or 3 are inconsistent, the standby CPU changes to STOP mode and outputs an error message.

If 4. is inconsistent, the master CPU copies the user program from its load memory in RAM to the standby CPU.

The user program stored in load memory on the FLASH card is not transferred.
It must be identical before initiating link-up.

Link-up with master/standby changeover

STEP 7 supports the following options:

- "Switch to CPU with modified configuration"
- "Switch to CPU with expanded memory configuration"
- "Switch to CPU with altered operating system"
- "Switch to CPU with modified hardware release"
- "Switch to CPU via only one intact redundant link"

Switch to CPU with altered configuration

You may have modified the following elements on the standby CPU:

- The hardware configuration
- The type of load memory (for example, you have replaced a RAM card with a FLASH card). The new load memory may be larger or smaller than the old one.

The master does not transfer any blocks to the standby during the link-up. For detailed information, refer to section Switch to CPU with modified configuration or expanded memory configuration (Page 110).

For information on the required steps, based on the scenarios described above (alteration of the hardware configuration, or of the type of memory for load memory), refer to section Failure and replacement of components during operation (Page 201).

Note

Event though you may not have modified the hardware configuration or the type of load memory on the standby CPU, a master/standby changeover is carried out and the previous master CPU changes to STOP.

Switch to CPU with expanded memory configuration

You may have expanded the load memory on the standby CPU. The memory media for storing load memory must be identical, i.e. either RAM cards or FLASH cards. If you expanded with FLASH cards, their contents must be identical.

During the link-up, the system transfers the user program blocks (OBs, FCs, FBs, DBs, SDBs) from load memory and work memory of the master to the standby CPU. Exception: If the load memory modules are FLASH cards, the system only transfers the blocks from work memory.

For information on changing the type of memory module or on load memory expansions, refer to section Changing the CPU memory configuration (Page 266).

NOTICE
Assuming you have changed the load memory type or modified the operating system on the standby CPU, this CPU does change to RUN, but returns to STOP and entry to the diagnostic buffer. If you have not expanded load memory on the standby CPU, this CPU does not change to RUN, but returns to STOP and writes an entry to the diagnostic buffer. The system does not perform a master/standby changeover, and the previous master CPU remains in RUN.

9.3.2 Update sequence

What happens during updating?

The execution of communication functions and OBs is restricted section by section during updating. Likewise, all the dynamic data (content of the data blocks, timers, counters and memory markers) are transferred to the standby CPU.

Update procedure:

1. Until the update is completed, all asynchronous SFCs which access the I/O modules (SFCs 13, 51, 52, 53, 55 to 59) initiate a "negative" acknowledgment with the return values W#16#80C3 (SFCs 13, 55 to 59) or W#16#8085 (SFC 51). When these values are returned, the jobs should be repeated by the user program.
2. Message functions are delayed until the update is completed (see list below).
3. The execution of the OB 1 and of all OBs up to priority class 15 is delayed.

   In the case of cyclic interrupts, the generation of new OB requests is disabled, so no new cyclic interrupts are stored and as a result no new request errors occur.

   The system waits until the update is completed, and then generates and processes a maximum of one request per cyclic interrupt OB. The time stamp of delayed interrupts can not be evaluated.
4. Transfer of all data block contents modified since link-up.
5. The following communication requests are acknowledged negatively:
   - Reading/writing data records using OCM functions
   - Reading diagnostic information using STEP 7
   - Disabling and enabling messages
   - Logon and logoff for messages
   - Acknowledgement of messages
6. The system returns a negative acknowledgment of initial calls of communication functions which manipulate the contents in RAM. See also *System Software for S7-300/400, System and Standard Functions*. All remaining communication functions are executed with delay, after the update is completed.
7. The system disables the generation of new requests of all OBs of priority class >15, so new interrupts are not saved and as a result do not generate any request errors.

   Queued interrupts are not requested again and processed until the update is completed. The time stamp of delayed interrupts can not be evaluated.

   The system no longer executes the user program or updates the I/O.
8. It generates the start event for the cyclic interrupt OB with special handling if its priority class is >15, and executes this OB as required.

Note

The cyclic interrupt OB with special handling is particularly important in situations where you need to address certain modules or program elements within a specific time. This is a typical scenario in fail-safe systems. For details, refer to the *S7-400F and S7-400FH Programmable Controllers* and *S7-300 Programmable Controllers, Fail-safe Signal Modules* manuals.

---

9. Transfer of outputs and of all data block contents modified again. Transfer of timers, counters, memory markers and inputs. Transfer of the diagnostics buffer.

   During this data synchronization, the system interrupts the clock pulse for cyclic interrupts, time-delay interrupts and S7 timers. This results in the loss of any synchronism between cyclic and time-of-day interrupts.

10. Lift all restrictions. Delayed interrupts and communication functions are executed. All OBs are executed again.

    A constant cycle time compared with previous calls can no longer be guaranteed for delayed cyclic interrupt OBs.

    Note

    Process and diagnostics interrupts are stored by the I/O. Such interrupt requests issued by distributed I/O modules are executed when the block is re-enabled. Any such requests by central I/O modules can only be executed provided the same interrupt request did not occur repeatedly while the status was disabled.

If the PG/ES requested a master/standby changeover, the previous standby CPU assumes master mode and the previous master CPU goes into STOP when the update is completed. Both CPUs will otherwise go into RUN (redundant system state) and execute the user program in synchronism.

When there is a master/standby changeover, in the first cycle after the update OB 1 is assigned a separate identifier (see *System Software for S7-300/400, System and Standard Functions* reference manual). For information on other aspects resulting from modifying the configuration, refer to section Switch to CPU with modified configuration or expanded memory configuration (Page 110).

Delayed message functions

The listed SFCs, SFBs and operating system services trigger the output of messages to all logged-on partners. These functions are delayed after the start of the update:

- SFC 17 "ALARM_SQ", SFC 18 "ALARM_S", SFC 107 "ALARM_DQ", SFC 108 ALARM_D"
- SFC 52 "WR_USMSG"
- SFB 31 "NOTIFY_8P", SFB 33 "ALARM", SFB 34 "ALARM_8", SFB 35 "ALARM_8P", SFB 36 "NOTIFY", SFB 37 "AR_SEND"
- Process control messages
- System diagnostics messages

From this time on, any requests to enable and disable messages by SFC 9 "EN_MSG" and SFC 10 "DIS_MSG" are rejected with a negative return value.

Communication functions and resulting jobs

After it has received one of the jobs specified below, the CPU must in turn generate communication jobs and output them to other modules. These include, for example, jobs for reading or writing parameter data records from/to the distributed I/O. These jobs are rejected until the update is completed.

- Reading/writing data records using OCM functions
- Reading data records using SSL information
- Disabling and enabling messages
- Logon and logoff for messages
- Acknowledgement of messages

Note

The last three of the functions listed are registered by a WinCC system, and automatically repeated when the update is completed.

9.3.3 Switch to CPU with modified configuration or expanded memory configuration

Switch to CPU with modified configuration

You may have modified the following elements on the standby CPU:

- The hardware configuration
- The type of memory module for load memory. You may have replaced a RAM card with a FLASH card for example. The new load memory may be larger or smaller than the old one.

For information on steps required in the scenarios mentioned above, refer to section Failure and replacement of components during operation (Page 201).

Note

Even though you have not modified the hardware configuration or the type of load memory on the standby CPU, there is nevertheless a master/standby changeover and the previous master CPU changes to STOP.

Note

If you have downloaded connections using NETPRO, you can no longer change the memory type of the load memory from RAM to FLASH.

When you initiate a link-up and update operation with the "Switch to CPU with modified configuration" option in STEP 7, the system reacts as follows with respect to handling of the memory contents.

Load memory

It does not copy the content of load memory from the master to the standby CPU.

RAM

The following components are transferred from the RAM of the master CPU to the standby CPU:

- Contents of all data blocks assigned the same interface time stamp in both load memories and having the attributes "read only" and "unlinked".
- Data blocks generated in the master CPU by SFCs.

  The DBs generated in the standby CPU by means of SFC are deleted.

  If a data block with the same number is also found in the load memory of the standby CPU, link-up is cancelled with an entry in the diagnostics buffer.
- Process images, timers, counters and memory markers
- Diagnostics buffer

  If the configured size of the diagnostics buffer of the standby CPU is smaller than that of the master CPU, only the number of entries configured for the standby CPU are transferred. The most recent entries are selected from the master CPU.

If there is insufficient memory, link-up is cancelled with an entry in the diagnostics buffer.

The status of SFB instances of S7 Communication contained in modified data blocks is restored to the status prior to their initial call.

Note

When changing over to a CPU with modified configuration, the size of load memories in the master and standby may be different.

Switch to CPU with expanded memory configuration

You may have expanded the load memory on the standby CPU. The memory media for storing load memory must be identical, i.e. either RAM cards or FLASH cards. If you expanded with FLASH cards, their contents must be identical.

NOTICE
Assuming you have implemented a different type of load memory module or operating system on the standby CPU, this CPU does not go into RUN, but rather returns to STOP and writes a corresponding message to the diagnostics buffer. Assuming you have not expanded load memory on the standby CPU, this CPU does not go into RUN, but rather returns to STOP and writes a corresponding message to the diagnostics buffer. The system does not perform a master/standby changeover, and the previous master CPU remains in RUN.

For information on changing the type of memory module or on load memory expansions, refer to section Failure and replacement of components during operation (Page 201).

When you initiate a link-up and update with the "Switch to CPU with expanded memory configuration" option in STEP 7, the system reacts as follows with respect to the handling of memory contents.

RAM and load memory

During the link-up, the system transfers the user program blocks (OBs, FCs, FBs, DBs, SDBs) from load memory of the master to RAM on the standby CPU. Exception: If the load memory modules are FLASH cards, the system only transfers the blocks from work memory.

9.3.4 Disabling link-up and update

Link-up and update entails a cycle time extension. This includes a period during which the I/O is not updated; see section Time monitoring (Page 114). Make allowances for this feature in particular when using distributed I/Os and on master/standby changeover after updating (that is, when modifying the configuration in Run).

CAUTION
Always perform link-up and update operations when the process is not in a critical state.

You can set specific start times for link-up and update operations at SFC 90 "H_CTRL". For detailed information on this SFC, refer to the *System Software for S7-300/400, System and Standard Functions*) manual.

NOTICE
If the process generally tolerates cycle time extensions, you do not need to call SFC 90 "H_CTRL". The CPU does not perform a self-test during link-up and updating. In a fail-safe system, you should therefore avoid any excess delay times for the update operation. For more details, refer to the *S7-400F and S7-400FH Programmable Controllers* manual.

Example of a time-critical process

A slide block with a 50 mm cam moves on an axis at a constant velocity v = 10 km/h = 2.78 m/s = 2.78 mm/ms. A switch is located on the axis. So the switch is actuated by the cam for the duration of Δt = 18 ms.

In order to enable the CPU to detect the actuation of the switch, the disable time for priority classes >15 (see below for definition) must be clearly below 18 ms.

With respect to maximum inhibit times for operations of priority class > 15, STEP 7 only supports settings of 0 ms or between 100 and 60000 ms, so you need to work around this by taking one of the following measures:

- Shift the start time of link-up and updating to a time at which the process state is non-critical. Use SFC 90 "H_CTRL" to set this time (see above).
- Use a considerably longer cam and/or substantially reduce the approach velocity of the slide block to the switch.

9.4 Time monitoring

Program execution is interrupted for a certain time during updating. This secton is relevant to you if this period is critical in your process. If this is the case, configure one of the monitoring times described below.

During updating, the fault-tolerant system monitors the cycle time extension, communication delay and inhibit time for priority classes > 15 in order to ensure that their maximum values are not exceeded, and that the configured minimum I/O retention time is maintained.

NOTICE
If you have not defined any default values for the monitoring times, make allowance for the update in the cycle monitoring time. If this is the situation, the update is cancelled and the fault-tolerant system switches to single mode: The previous master CPU remains in RUN, and the standby CPU goes into STOP. You can either configure all the monitoring times or none at all.

You made allowances for the technological requirements in your configuration of monitoring times.

The monitoring times are described in detail below.

- Maximum cycle time extension
  - Cycle time extension: The cycle time extension is the time during the update in which neither OB 1 nor any other OBs up to priority class 15 are executed. The "normal" cycle time monitoring function is disabled within this time span.
  - Max. cycle time extension: The maximum cycle time extension represents the configured and permissible maximum.
- Maximum communication delay
  - Communication delay: The communication delay represents a time span within the update during which the CPU does not execute any communication functions. Note: The master CPU maintains all existing communication links.
  - Maximum communication delay: The maximum communication delay represents the configured and permissible maximum.
- Maximum inhibit time for priority classes > 15
  - Inhibit time for priority classes > 15: The time span within an update during which the CPU neither executes any OBs (and so any user program) nor any further I/O updates.
  - Maximum inhibit time for priority classes > 15: The maximum inhibit time for priority classes > 15 represents the configured and permissible maximum.

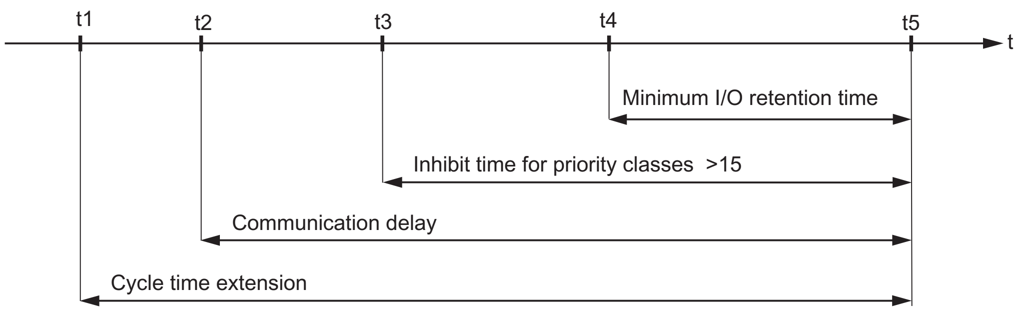
- Minimum I/O retention time:

  This represents the interval between copying of the outputs from the master CPU to the standby CPU and the time of the transition to the redundant system state or master/standby changeover (time at which the previous master CPU goes into STOP and the new master CPU goes into RUN). Both CPUs control the outputs within this period, in order to prevent the I/O from going down when the system performs an update with master/standby changeover.
  The minimum I/O retention time is of particular importance when updating with master/standby changeover. If you set the minimum I/O retention time to zero, the outputs could possibly shut down when you modify the system in Run.

The monitoring start times are indicated in the highlighted boxes in Figure 9-2. These times expire when the system enters the redundant state or on a master/standby changeover, i.e. on the transition of the new master to RUN when the update is completed.

The figure below provides an overview of the relevant update times.

Update:



t1: End of current OBs up to priority class 15
t2: Stop all communication functions
t3: End of watchdog interrupt OB with special handling
t4: End of copying of outputs to the standby CPU
t5: Redundant system status, or master/standby changeover

Figure 9-4 Meanings of the times relevant for updates

Reaction to timeouts

If one of the times monitored exceeds the configured maximum, the following procedure is started:

1. Cancel update
2. Fault-tolerant system remains in single mode, with the previous master CPU in RUN
3. Enter cause of cancelation in diagnostic buffer
4. Call OB 72 (with corresponding start information)

The standby CPU then evaluates its system data blocks again.
Then, but after at least one minute, the CPU tries again to perform the link-up and update. If still unsuccessful after a total of 10 retries, the CPU abandons the attempt. You yourself will then need to start the link-up and update again.

A monitoring timeout can be caused by:

- High interrupt load (for example from I/O modules)
- high communication load causing prolonged execution times for active functions
- In the final update phase, the system needs to copy large amounts of data to the standby CPU.

9.4.1 Time-based reaction

Time-based reaction during link-up

The influence of link-up operations on your plant control system should be kept to an absolute minimum. The current load on your automation system is therefore a decisive factor in the increase of link-up times. The time required for link-up is in particular determined by

- the communication load
- the cycle time

The following applies to no-load operation of the automation system:

Link-up runtime = size of load memory and work memories in MB x 1 s + base load

The base load is a few seconds.

Whenever your automation system is subject to high load, the memory-specific share may increase up to 1 minute per MB.

Time-based reaction during updating

The update transfer time is determined by the number and overall length of modified data blocks, rather than on the modified volume of data within a block. It is also determined by the current process status and the communication load.

As a simple approximation, we can interpret the maximum inhibit time to be configured for priority classes > 15 as a function of the data volume in RAM. The volume of code in RAM is irrelevant.

9.4.2 Determining the monitoring times

Determination using STEP 7 or formulas

STEP 7 automatically calculates the monitoring times listed below for each new configuration. You can also calculate these times using the formulas and procedures described below. They are equivalent to the formulas provided in STEP 7.

- Maximum cycle time extension
- Maximum communication delay
- Maximum inhibit time for priority classes
- Minimum I/O retention time

You can also start automatic calculation of monitoring times with Properties CPU > H Parameters in HW Config.

Monitoring time accuracy

Note

The monitoring times determined by STEP 7 or by using formulas merely represent recommended values.

These times are based on a fault-tolerant system with two communication partners and an average communication load.

Your system profile may differ considerably from those scenarios, so observe the following rules.

- The cycle time extension factor may increase sharply at a high communication load.
- Any modification of the system in operation may lead to a significant increase in cycle times.
- Any increase in the number of programs executed in priority classes >15 (in particular those of communication blocks) automatically increases the communication delay and cycle time extension.
- You can even undercut the calculated monitoring times in small high-performance systems.

Configuration of the monitoring times

When configuring monitoring times, always make allowances for the following dependencies; conformity is checked by STEP 7:

Max. cycle time extension
> max. communication delay
> (max. disable time for priority classes > 15)
> min. I/O retention time

If you have configured different monitoring times in the CPUs and perform a link-up and update operation with master/standby changeover, the system always applies the higher of the two values.

Calculating the minimum I/O retention time (T_{PH})

The following applies to the calculation of the minimum I/O retention time:

- with central I/O: T_{PH} = 30 ms
- with distributed I/O: $T_{PH} = 3 \times T_{TRmax}$

  where T_{TRmax} = maximum target rotation time
  all DP master systems of the fault-tolerant station

When using central and distributed I/Os, the resultant minimum I/O retention time is:

T_{PH} = MAX (30 ms, $3 \times T_{TRmax}$)

The following figure shows the correlation between the minimum I/O hold time and the maximum disable time for priority classes > 15.

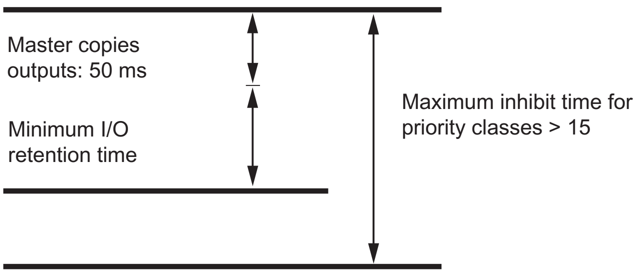


Figure 9-5 Correlation between the minimum I/O hold time and the maximum disable time for priority classes > 15

Note the following condition:

50 ms + minimum I/O hold time ≤
(maximum disable time for priority classes > 15)

It follows that a high minimum I/O hold time can determine the maximum disable time for priority classes > 15.

Calculating the maximum disable time for priority classes > 15 (T_{P15})

The maximum disable time for priority classes > 15 is determined by four main factors:

- As shown in Figure 8-2, all the contents of data blocks modified since the last copy to the standby CPU are transferred to the standby CPU again when the update is completed. **The number and structure of the DBs** you write to in the high-priority classes is a decisive factor in the duration of this operation, and so in the maximum disable time for priority classes > 15. Relevant information is available in the remedies described below.
- In the final update phase, all OBs are either delayed or disabled. To avoid any unnecessary extension of the maximum disable time for priority classes > 15 due to unfavorable programming, you should always process the time-critical I/O components in a **selected cyclic interrupt**. This is particularly relevant in fail-safe user programs. You can configure this cyclic interrupt in your project and execute it automatically immediately after the start of the maximum disable time for priority classes > 15, provided you have assigned it a priority class > 15.
- In link-up and update operations with master/standby changeover (see section Link-up sequence (Page 105)), you also need to change over the active communication channel on the switched DP slaves when the update is completed. This operation prolongs the time within which valid values can neither be read nor output. How long this takes is decided by your **hardware configuration**.
- The **technological conditions in your process** also decide how long an I/O update can be delayed. This is particularly important in time-monitored processes in fail-safe systems.

Note

For details, refer to the *S7-400F and S7-400FH Automation Systems* and *S7-300 Automation Systems, Fail-safe Signal Modules* manuals. This applies in particular to the internal execution times of fail-safe modules.

---

1. Based on the bus parameters in STEP 7, for each DP master system define
   - T_{TR} for the DP master system
   - DP changeover time (referred to below as T_{DP_UM})
2. Based on the technical data of the switched DP slaves, for each DP master system, define
   - the maximum changeover time of the active communication channel (referred to below as T_{SLAVE_UM}).
3. Based on the technological defaults of your system, define
   - the maximum permissible time during is no update of your I/O modules (referred to below as T_{PTO}).
4. Based on your user program, define
   - The cycle time of the highest-priority or selected (see above) cyclic interrupt (T_{WA})
   - The execution time of your program in this cyclic interrupt (T_{PROG})

5. For each DP master system this results in

   T_{P15} (DP master system) = T_{PTO} - (2 x T_{TR} + T_{WA} + T_{PROG} + T_{DP_UM} + T_{SLAVE_UM}) [1]

NOTICE
If T_{P15}(DP master system) < 0, stop the calculation here. Possible remedies are shown below the following example calculation. Make suitable changes and then restart the calculation at 1.

6. Select the minimum of all T_{P15} (DP master system) values.

   This time is then known as TP15_HW.

7. Define the share of the maximum disable time for I/O classes > 15 determined by the minimum I/O hold time (T_{P15_OD}):

   T_{P15_OD} = 50 ms + min. I/O hold time [2]

NOTICE
If T_{P15_OD} > T_{P15_HW}, stop the calculation here. Possible remedies are shown below the following example calculation. Make suitable changes and then restart the calculation at 1.

8. Using the information in section Link-up sequence (Page 105), calculate the share of the maximum disable time for priority classes > 15 defined by the user program (T_{P15_AWP}).

NOTICE
If T_{P15_AWP} > T_{P15_HW}, stop the calculation here. Possible remedies are shown below the following example calculation. Make suitable changes and then restart the calculation at 1.

9. The recommended value for the maximum disable time for priority classes > 15 is now obtained from:

   T_{P15} = MAX (T_{P15_AWP}, T_{P15_OD}) [3]

Example of the calculation of T_{P15}

In the next steps, we take an existing configuration and we define the maximum permitted time during an update during which the operating system does not execute any programs or update the I/O.

We assume two DP master systems: DP master system_1 is "connected" to the CPU via the MPI/DP interface of the CPU, and DP master system_2 via an external DP master interface.

1. Based on the bus parameters in STEP 7:

   T_{TR_1} = 25 ms

   T_{TR_2} = 30 ms

   $T_{DP\_UM\_1}$ = 100 ms

   $T_{DP\_UM\_2}$ = 80 ms

2. Based on the technical data of the DP slaves used:

   $T_{SLAVE\_UM\_1}$ = 30 ms

   $T_{SLAVE\_UM\_2}$ = 50 ms

3. Based on the technological demands of your system:

   T_{PTO_1} = 1250 ms

   T_{PTO_2} = 1200 ms

4. Based on the user program:

   T_{WA} = 300 ms

   T_{PROG} = 50 ms

5. Based on the formula [1]:

   T_{P15} (DP master system_1)

   = 1250 ms - (2 x 25 ms + 300 ms + 50 ms + 100 ms + 30 ms) = 720 ms

   T_{P15} (DP master system_2)

   = 1200 ms - (2 x 30 ms + 300 ms + 50 ms + 80 ms + 50 ms) = 660 ms

Check: since $T_{P15} < 0$, continue with

1. T_{P15_HW} = MIN (720 ms, 660 ms) = 660 ms
2. Based on the formula [2]:

T_{P15_OD} = 50 ms + T_{PH} = 50 ms + 90 ms = 140 ms

Check: since T_{P15_OD} = 140 ms < T_{P15_HW} = 660 ms continue with

1. Based on section 7.4.4 with 170 KB of user program data:

   T_{P15_AWP} = 194 ms

Check: as T_{P15_AWP} = 194 ms < T_{P15_HW} = 660 ms continue with

1. Based on formula [3], we now obtain the recommended maximum disable time for priority classes > 15:

T_{P15} = MAX (194 ms, 140 ms)

T_{P15} = 194 ms

This means that by setting a maximum disable time of 194 ms for priority classes > 15 in STEP 7, you can ensure that any signal changes during the update are detected with a signal duration of 1250 ms or 1200 ms.

Remedies if it is not possible to calculate T_{P15}

If no recommendation results from calculation of the maximum inhibit time for priority classes > 15, you can remedy this by taking various measures:

- Reduce the cyclic interrupt cycle of the configured cyclic interrupt.
- If T_{TR} times are particularly high, distribute the slaves across several DP master systems.
- Increase the transfer rate on the affected DP master systems.
- Configure the DP/PA Links and Y Links in separate DP master systems.
- If there is a great difference in changeover times on the DP slaves, and so (generally) great differences in T_{PTO}, distribute the slaves involved across several DP master systems.
- If you do not expect any significant load caused by interrupts or parameter assignment in the various DP master systems, you can also reduce the calculated T_{TR} times by around 20% to 30%. However, this increases the risk of a station failure in the distributed I/O.
- The time value T_{P15_AWP} represents a guideline and depends on your program structure. You can reduce it by taking the following measures, for example:
  - Save data that changes often in different DBs from data that does not change as often.
  - Assign the DBs a smaller length in work memory.

If you reduce the time T_{P15_AWP} without taking the measures described, you run the risk that the update operation will be aborted due to a monitoring timeout.

Calculation of the maximum communication delay

Use the following formula:

Maximum communication delay =
4 x (maximum inhibit time for priority classes > 15)

Decisive factors for this time are the process status and the communication load in your system. This can be understood as the absolute load, or as the load relative to the size of your user program. You may have to adjust this time.

Calculation of the maximum cycle time extension

Its is advisable to use the following formula:

Maximum cycle time extension =
10 x (maximum disable time for priority classes > 15)

Decisive factors for this time are the process status and the communication load in your system. This can be understood as the absolute load, or as the load relative to the size of your user program. You may have to adjust this time.

See also

Performance values for link-up and update (Page 125)

9.4.3 Performance values for link-up and update

User program share T_{P15_AWP} of the maximum inhibit time for priority classes > 15

The user program share T_{P15_AWP} of the maximum inhibit time for priority classes > 15 can be calculated using the following formula:

T_{P15_AWP} in ms = 0.7 x size of DBs in work memory in KB + 75

The table below shows the derived times for some typical values in work memory data.

Table 9-3 Typical values for the user program part

Work memory data	T_{P15_AWP}
500 KB	220 ms
1 MB	400 ms
2 MB	0.8 s
5 MB	1.8 s
10 MB	3.6 s

The following assumptions were made for this formula:

- 80% of the data blocks are modified prior to delaying the interrupts of priority classes > 15.
  In particular for fail-safe systems, this calculated value must be more precise to avoid any timeout of driver blocks (see section Determining the monitoring times (Page 118)).
- For active or queued communication functions, allowance is made for an update time of approximately 100 ms per MB in the work memory occupied by data blocks.
  Depending on the communication load of your automation system, you will need to add or deduct a value when you set T_{P15_AWP}.

9.4.4 Influences on time-based reaction

The period during which no I/O updates take place is primarily determined by the following influencing factors:

- the number and size of data blocks modified during the update
- the number of instances of SFBs in S7 communication, and of SFBs for generating block-specific messages
- system modifications in operation
- settings by means of dynamic volume frameworks
- expansion of distributed I/Os (a lower Baud rate and higher number of slaves increases the time required for I/O updates).

In the worst case, this period is extended by the following amounts:

- maximum watchdog interrupt cycle used
- duration of all watchdog interrupt OBs
- duration of high-priority interrupt OBs executed until the start of interrupt delays

Explicit delay of the update

Delay the update using SFC 90 "H_CTRL", and re-enable only when the system state shows less communication or interrupt load.

⚠ CAUTION
The update delay increases the time of single mode operation of the fault-tolerant system.

9.5 Special features in link-up and update operations

Requirement for input signals during the update

Any process signals read previously are retained and not included in the update. The CPU only recognizes changes of process signals during the update if the changed state remains after the update is completed.

The CPU does not detect pulse signals (signal transitions "0 → 1 → 0" or "1 → 0 →1") which are generated during the update.

You should therefore ensure that the interval between two signal transitions (pulse period) is always greater than the required update period.

Communication links and functions

Connections on the master CPU are not be shut down. However, the CPU does not execute any associated communication requests until the update is completed. They are queued for execution as soon as one of the following cases occurs:

- the update is completed, and the system is in the redundant state.
- the update and master/standby changeover are completed, the system is in single mode.
- the update was aborted (due to timeout, for example), and the system has returned to single mode.

An initial call of communication blocks is not possible during the update.

CPU memory reset request on aborted link-up

If the link-up operation is aborted while the content of load memory is being copied from the master to the standby CPU, the standby CPU requests a memory reset. This indicated in the diagnostics buffer by event ID W#16#6523.

10 Using I/Os in S7–400H

10.1 Using I/Os in S7–400H

This section provides an overview of the different I/O installations on the S7-400H automation system and their availability. It also provides information on configuration and programming of the selected I/O installation.

10.2 Introduction

I/O installation types

In addition to the power supply module and CPUs, which are always redundant, the operating system supports the following I/O installations:

I/O type	Installation	Availability
Digital input	Single-channel one-sided Single-channel switched Dual-channel redundant	normal enhanced high
Digital output	Single-channel one-sided Single-channel switched Dual-channel redundant	normal enhanced high
Analog input	Single-channel one-sided Single-channel switched Dual-channel redundant	normal enhanced high
Analog output	Single-channel one-sided Single-channel switched Dual-channel redundant	normal enhanced high

A dual-channel redundant configuration at user level is also possible. You nevertheless need to implement the high availability in the user program (see section Other options for connecting redundant I/Os (Page 164)).

Addressing

No matter whether you are using a single-channel, one-sided or switched I/O, you always access the I/O at the same address.

Limits of I/O configuration

If there are insufficient slots in the central racks, you can add up to 20 expansion units to the S7-400H configuration.

Module racks with even numbers are always assigned to central unit 0, and racks with odd numbers are assigned to central unit 1.

For applications with distributed I/O, each of the subsystems supports the connection of up to 12 DP master systems (two DP master systems on the integrated interfaces of the CPU and 10 via external DP master systems).

The integrated MPI/DP interface supports the operation of up to 32 slaves. You can connect up to 125 distributed I/O devices to the integrated DP master interface and to the external DP master systems.

10.3 Using single-channel, one-sided I/Os

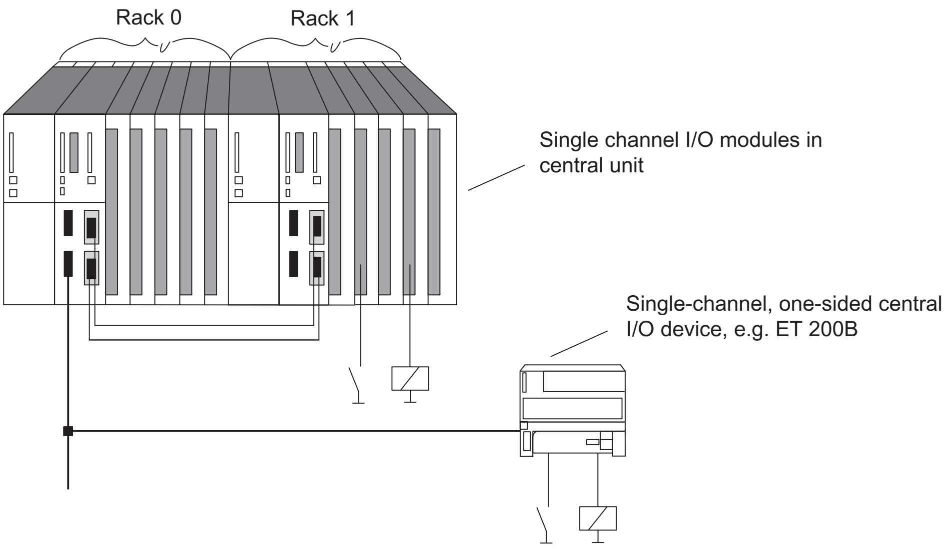
What is single-channel one-sided I/O?

In the single-channel one-sided configuration, the input/output modules exist only once (single-channel). The I/O modules are located in only one subsystem, and are always addressed by it.

A single-channel, one-sided I/O configuration is possible in

- CPUs and expansion units
- distributed I/O devices

An installation with single-channel, one-sided I/O is useful for the operation of single I/O channels up to system components which only require the standard availability.



Single-channel, one-sided I/O configuration

Single-channel, one-sided I/O and the user program

When the system is in redundant mode, the data read from one-sided components (such as digital inputs) is transferred automatically to the second subsystem.

When the transfer is completed, the data read from the single-channel one-sided I/O is available on both subsystems and can be evaluated in their identical user programs. For data processing in the redundant system state, it is irrelevant whether the I/O is connected to the master or to the standby CPU.

In single mode, access to one-sided I/O assigned to the partner subsystem is not possible. Remember to take this into account in your program: Make sure that you only assign functions to the single-channel one-sided I/O that can only be executed conditionally. This ensures that specific I/O access functions are only called in the redundant system state, and when the relevant subsystem is in single mode.

NOTICE
The user program also has to update the process image for single-channel, one-sided output modules when the system is in single mode (direct access, for example). If you use process image partitions, the user program must update them (SFC27 "UPDAT_PO") in OB 72 (recovery of redundancy). The system would otherwise initialize the single-channel one-sided output modules of the standby CPU with the old values after the system change to redundant mode.

Failure of the single-channel one-sided I/O

The fault-tolerant system with single-channel, one-sided I/O reacts to errors just like a standard S7-400 system, in other words:

- The I/O is no longer available after it fails.
- If the subsystem to which the I/O is connected fails, the entire process I/O of this subsystem is no longer available.

10.4 Using single-channel switched I/Os

What is single-channel switched I/O?

In the single-channel switched configuration, the input/output modules are present singly (single-channel).

In redundant mode, these can addressed by both subsystems.

In single mode, the master subsystem can always address **the entire switched I/O** (in contrast to one-sided I/O).

The system supports single-channel switched I/O configurations containing an ET 200M distributed I/O module with active backplane bus and a redundant PROFIBUS DP slave interface module.

You can use the following interfaces:

Table 10-1 Interfaces for the use of single-channel switched I/O

Interface	Order number
IM 153–2	6ES7153–2BA81–0XB0 6ES7153–2BA02–0XB0 6ES7153–2BA01–0XB0 6ES7153–2BA00–0XB0
IM 153–2FO	6ES7153–2AB02–0XB0 6ES7153–2AB01–0XB0 6ES7153–2AB00–0XB0 6ES7153–2AA02–0XB0

Each S7-400H subsystem is interconnected with one of the two DP slave interfaces of the ET 200M via a DP master interface.

PROFIBUS PA can be interconnected with a redundant system by DP/PA link.

You can use the following DP/PA links:

DP/PA link	Order number
IM 157	6ES7157–0BA82–0XA0 6ES7157–0AA82–0XA0 6ES7157–0AA81–0XA0 6ES7157–0AA80–0XA0
ET 200M as DP/PA link with	6ES7153–2BA02–0XB0 6ES7153–2BA01–0XB0 6ES7153–2BA81–0XB0

A single-channel DP master system can be interconnected with a redundant system by means of Y link.
Supported IM 157 Y link: 6ES7197-1LB00 0XA0

The single-channel switched I/O configuration is recommended for system components which tolerate the failure of individual modules within the ET 200M.

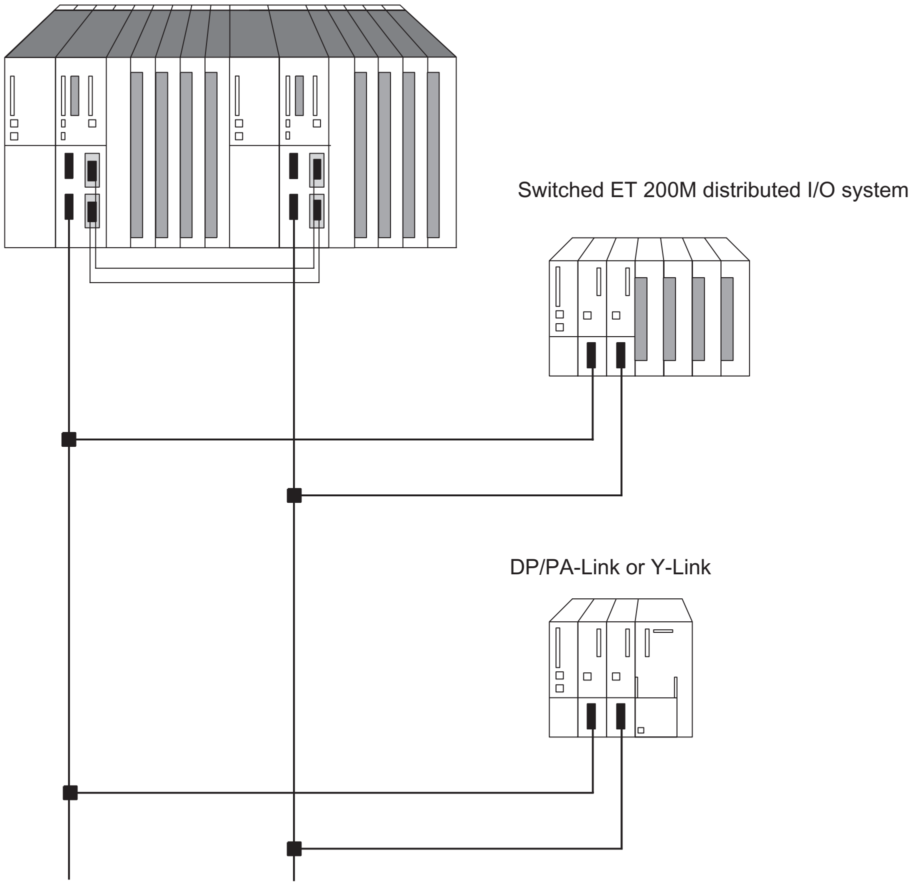


Figure 10-1 Single-channel, switched ET 200M distributed I/O

Rule

A single-channel, switched I/O configuration must always be symmetrical, in other words:

- The H CPU and other DP masters must be installed in the same slots in both subsystems (for example, slot 4 on both subsystems), or
- The DP masters must be connected to the same integrated interface in both subsystems (for example, to the PROFIBUS DP interfaces of both H CPUs).

Single-channel, switched I/O and the user program

In redundant mode, any subsystem can, in principle, access single-channel switched I/O. The data is automatically transferred via the synchronization link and compared. An identical value is available to the two subsystems at all times owing to the synchronized access.

The fault-tolerant system uses only one of the interfaces at any given time. The active interface is indicated by the ACT LED on the corresponding IM 153-2 or IM 157.

The path via the currently active interface (IM 153-2 or IM 157) is called the **active channel** and the path via the other interface as the **passive channel**. The DP cycle is always active on both channels. However, only the input and output values of the active channel are processed in the user program or output to the I/O. The same applies to asynchronous activities, such as interrupt processing and the exchange of data records.

Failure of the single-channel, switched I/O

The fault-tolerant system with single-channel, switched I/O reacts to errors as follows:

- The I/O is no longer available after it fails.
- In certain failure situations (such as the failure of a subsystem, DP master system or DP slave interface module IM153-2 or IM 157; see Chapter Communication (Page 169)), the single-channel, switched I/O remains available to the process.
  This is achieved by a failover between the active and passive channel. This failover takes place separately for each DP station. A distinction is made between the following types of failure
  - Failures affecting only one station (such as failure of the DP slave interface module of the currently active channel)
  - Failures affecting all the stations of a DP master system.
    This includes unplugging of the DP master interface, shutdown of the DP master system (for example, RUN-STOP change on a CP 443-5) and short-circuits on the cable chain of a DP master system.

The following applies to each station affected by a failure: If both DP slave interface modules are currently functional and the active channel fails, the previously passive channel automatically becomes active. A redundancy loss is reported to the user program when OB 70 starts (event W#16#73A3).

If the problem is eliminated, the redundant mode is restored. This also starts OB 70 (event W#16#72A3). In this situation, there is no changeover between the active and passive channel.

If one channel has already failed, and the remaining (active) channel also fails, then there is a complete station failure. This starts OB 86 (event W#16#39C4).

Note

If the DP master interface module can detect failure of the entire DP master system (due to short-circuit, for example), it reports only this event ("Master system failure entering state" W#16#39C3). The operating system no longer reports individual station failures. This feature can be used to accelerate the failover between the active and passive channel.

Duration of a failover of the active channel

The maximum failover time is

DP error detection time + DP failover time + failover time of the DP slave interface module

You can determine the first two values from the bus parameters of your DP master system in STEP 7. You can obtain the last value from the manuals of the relevant DP slave interface module *(Distributed I/O ET 200M* and *DP/PA Bus Link*).

NOTICE
When using fail-safe modules, always set a monitoring time for each fail-safe module that is longer than the failover time of the active channel in the fault-tolerant system. If you ignore this rule, you risk failure of the fail-safe modules during the failover of the active channel.

NOTICE
The above calculation also includes the processing time in OB 70 or OB 86. Make sure that the processing time for a DP station **does not last longer than 1 ms**. In situations requiring extensive processing, exclude this processing from direct execution of the OBs mentioned. Note that the CPU can only detect a signal change if the signal duration is greater than the specified failover time. When there is a failover of the entire DP master, the failover time of the slowest component applies to all DP components. A DP/PA Link or Y Link usually determines the failover time and the associated minimum signal duration. We therefore recommend that you connect the DP/PA and Y Links to a separate DP master system. When using fail-safe modules, always set a monitoring time for each fail-safe module that is longer than the failover time of the active channel in the fault-tolerant system. If you ignore this, you risk failure of the fail-safe modules during the failover of the active channel.

Changeover of the active channel during link-up and updating

During link-up and update with master/standby changeover (see section Link-up sequence (Page 105)) the active and passive channels are changed over on all stations of the switched I/O. At the same time OB 72 is called.

Bumpless changeover of the active channel

To prevent the I/O failing temporarily or outputting substitute values during the changeover between the active and passive channel, the DP stations of the switched I/O put their outputs on hold until the changeover is completed and the new active channel has taken over.

To ensure that total failures of a DP station are detected during the changeover, the changeover is monitored by the various DP stations and by the DP master system.

Provided the minimum I/O hold time is set correctly (see section Time monitoring (Page 114)), no interrupts or data records will be lost due to a changeover. There is an automatic repetition when necessary.

System configuration and project engineering

You should allocate switched I/O with different failover times to separate chains. This, for example, simplifies the calculation of monitoring times.

10.5 Connecting redundant I/Os

10.5.1 Connecting redundant I/Os

What is redundant I/O?

Input/Output modules are considered redundant when the system contains two sets of each module, and these are configured and operated as redundant pairs. The use of redundant I/O provides the highest degree of availability, because the system tolerates the failure of a CPU or of a signal module.

Configurations

The following redundant I/O configurations are supported:

1. Redundant signal modules in the CPUs and expansion units
   The signal modules are installed in pairs in the CPU 0 and CPU 1 subsystems.

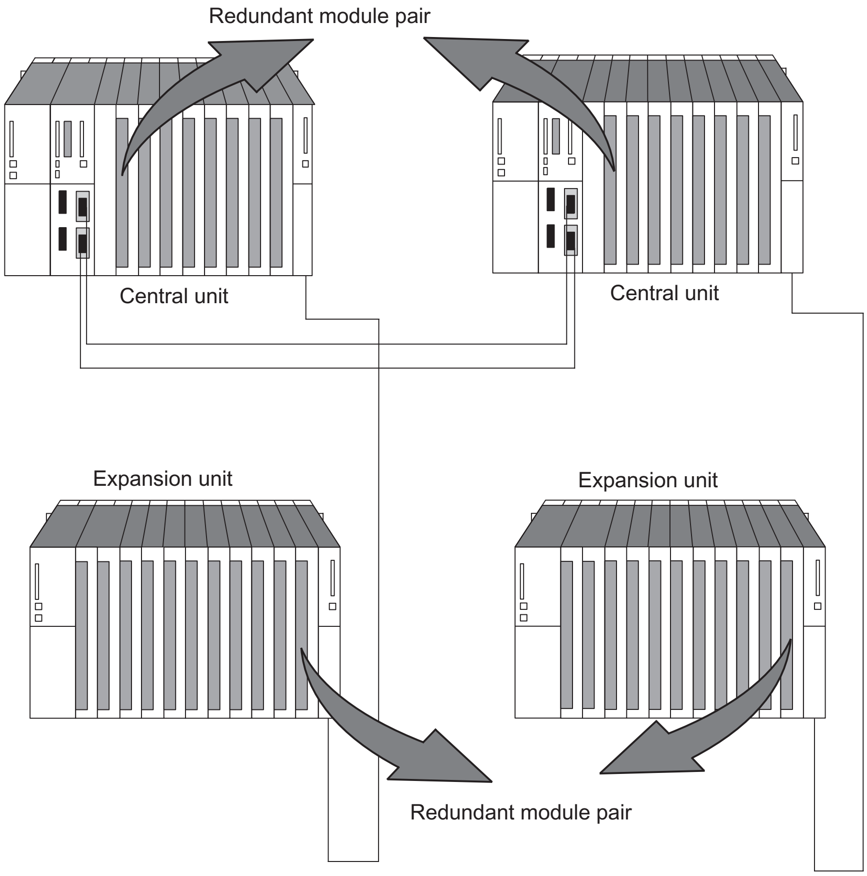


Figure 10-2 Redundant I/O in central and expansion units

2. Redundant I/O in the one-sided DP slave

   To achieve this, the signal modules are installed in pairs in ET 200M distributed I/O devices with active backplane bus.

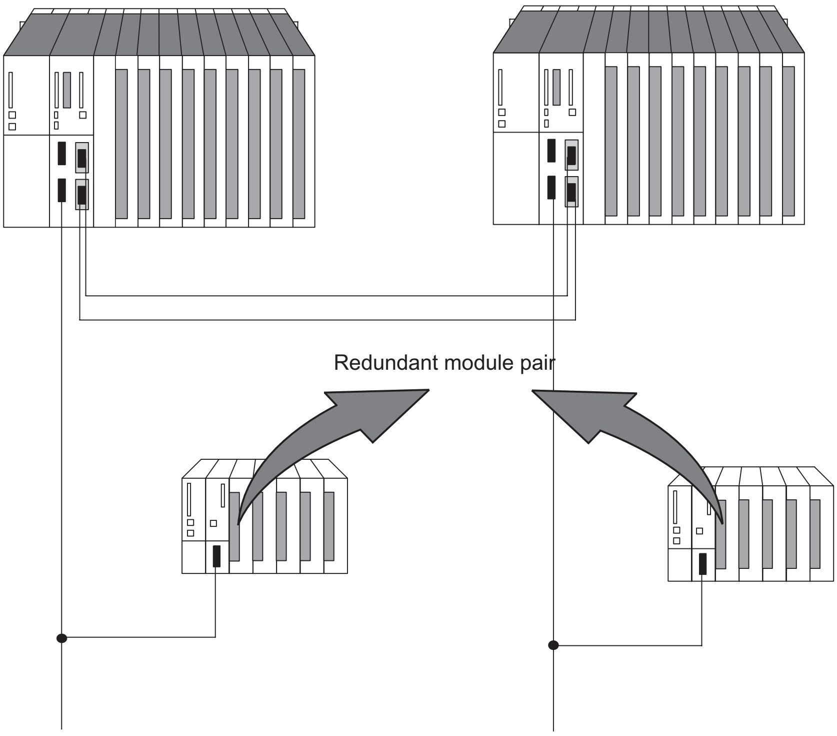


Figure 10-3 Redundant I/O in the one-sided DP slave

3. Redundant I/O in the switched DP slave

   To achieve this, the signal modules are installed in pairs in ET 200M distributed I/O devices with active backplane bus.

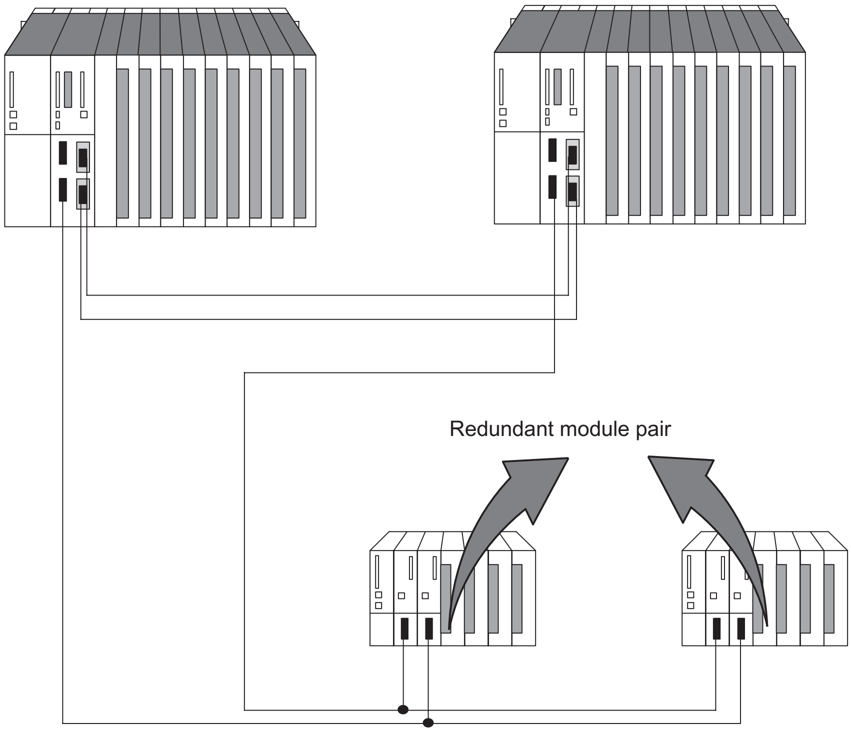


Figure 10-4 Redundant I/O in the switched DP slave

4. Redundant I/O connected to a fault-tolerant CPU in single mode

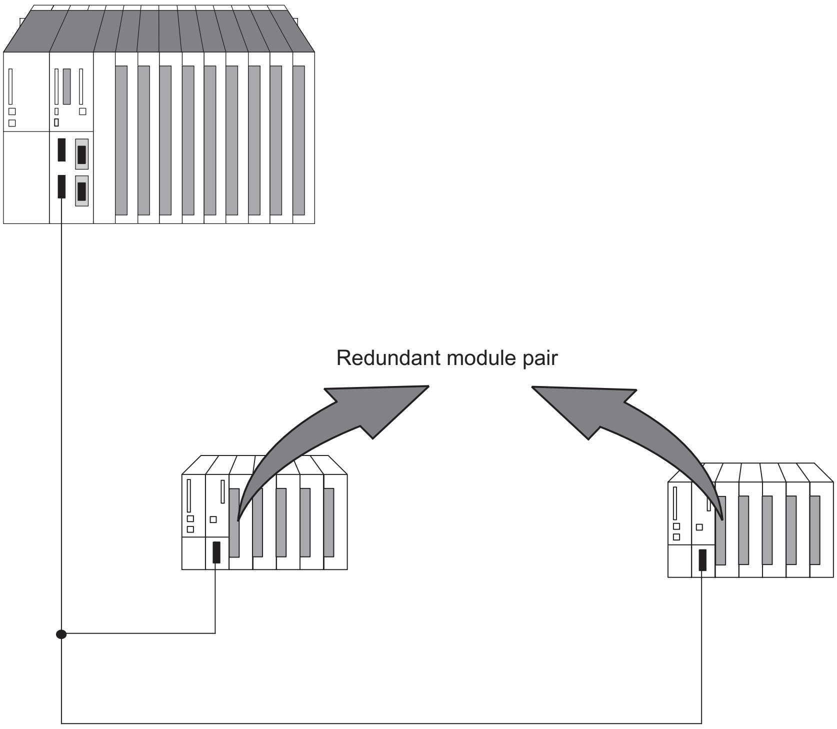


Figure 10-5 Redundant I/O in single mode

Principle of channel group redundancy

Channel errors, whether due to discrepancy or diagnostic interrupt (OB82), do not bring about the passivation of the respective channel group. Depassivation depassivates all channels involved as well as the modules passivated due to module errors. Channel group passivation significantly increases availability in the following situations:

- Relatively frequent encoder failures
- Repairs that take a long time
- Multiple channel errors on one module

Depending on the module, a channel group receives one single channel, one group of several channels or all channels of the module. You can therefore operate all the redundant usable modules in channel group redundancy.

Refer to FAQ under http://support.automation.siemens.com/ for an up-to-date list of the redundant usable modules.

Note

Operating redundant modules

If you are operating signal modules for the first time, use the channel group redundancy. This ensures the highest possible flexibility when using redundant modules.

Principle of module-oriented redundancy

Redundancy always applies to the entire module, rather than to individual channels. When a channel error occurs in the first redundant module, the entire module and its channels are passivated. If an error occurs on another channel on the second module before the first error has been eliminated and the first module has been depassivated, this second error cannot be handled by the system.

You can check which modules you can operate in module redundancy in the section "Signal modules for redundancy".

Refer to FAQ under http://support.automation.siemens.com/ for an up-to-date list of the redundant usable modules.

Principle of channel-oriented redundancy

Channel errors, whether due to discrepancy or diagnostic interrupt (OB82), do not lead to the entire module being passivated. Instead, only the channel involved is passivated. Depassivation depassivates the channel involved as well as the modules passivated due to module errors.

You can check which modules you can operate with channel redundancy in the section "Signal modules for redundancy".

Refer to FAQ under http://support.automation.siemens.com/ for an up-to-date list of the redundant usable modules.

"Functional I/O redundancy" block libraries

The "Functional I/O redundancy" block libraries that support the redundant I/O each contain the following blocks:

- FC 450 "RED_INIT": Initialization function
- FC 451 "RED_DEPA": Initiate depassivation
- FB 450 "RED_IN": Function block for reading redundant inputs
- FB 451 "RED_OUT": Function block for controlling redundant outputs
- FB 452 "RED_DIAG": Function block for diagnostics of redundant I/O
- FB 453 "RED_STATUS": Function block for redundancy status information

Configure the numbers of the management data blocks for the redundant I/O in HW Config "Properties CPU -> H Parameter". Assign free DB numbers to these data blocks. The data blocks are created by FC 450 "RED_INIT" during CPU startup. The default setting for the numbers of the management data blocks is 1 and 2. These data blocks are not the instance data blocks of FB 450 "RED_IN" or FB 451 "RED_OUT".

The blocks you use for channel group redundancy are located in the "Redundant IO CGP V50" library.

The blocks you use for channel group redundancy are located in the "Redundant IO CGP V40" library.

The blocks you use for channel group redundancy are located in the "Redundant IO MGP V30" library.

You can open the libraries in the SIMATIC Manager with "File -> Open -> Libraries"

The functions and use of the blocks are described in the corresponding online help.

NOTICE
Block libraries Only use modules from one library. The simultaneous use of blocks from different libraries is not permitted. If you wish to replace one of the earlier libraries Redundant IO (V1) or Redundant IO CGP with the Redundant IO CGP V5.0, you must first of all edit your user program accordingly. Refer to the context-sensitive block help or the STEP 7 Readme

Switching to channel group redundancy

To activate channel group passivation, you have to stop the automation system (memory reset and reload user program in STOP).

Note the following points:

Mixing blocks from the various libraries in one CPU is not permitted and can lead to unpredictable behavior.

When converting a project, make sure that all library blocks named FB450-453 and FC450-451 have been deleted from the block folder and replaced by the blocks from Red-IO CGP V5.0. Perform this step in every relevant program. Compile and load your project.

Using the blocks

Before you use the blocks, configure the redundant modules as redundant in HW Config.

The OBs into which you need to link the various blocks are listed in the table below:

Block	OB
FC 450 "RED_INIT"	• OB 72 "CPU redundancy error" (only with H systems) FC 450 is only executed after start event B#16#33:"Standby-master changeover by operator". • OB 80 "Timeout error" (only in single mode) The FC 450 is only executed after the start event "Resume RUN after reconfiguring". • OB 100 "Restart" (the administration DBs are recreated, see the online help) • OB 102 "Cold restart"
FC 451 "RED_DEPA"	When you call FC 451 in OB 83 after inserting modules, this function allows an approximately 3-second delayed depassivation.
FB 450 "RED_IN"	• OB1 "Cyclic program" • OB 30 to OB 38 "Cyclic interrupt"
FB 451 "RED_OUT"	• OB1 "Cyclic program" • OB 30 to OB 38 "Cyclic interrupt"
FB 452 "RED_DIAG"	• OB 72 "CPU redundancy error" • OB 82 "Diagnostic interrupt" • OB 83 "Insert/remove module interrupt" • OB 85 "Program execution error"
FB 453 "RED_STATUS"	• OB1 "Cyclic program" (H systems only) • OB 30 to OB 38 "Cyclic interrupt"

To be able to address redundant modules using process image partitions in cyclic interrupts, the relevant process image partition must be assigned to this pair of modules and to the cyclic interrupt. Call FB 450 "RED_IN" in this cyclic interrupt before you call the user program. Call FB 451 "RED_OUT" in this cyclic interrupt after you call the user program.

The valid values that can be processed by the user program are always located at the lower address of both redundant modules. This means that only the lower address can be used by the application; the values of the higher address are not relevant for the application.

Note

Use of FB 450 "RED_IN" and 451 "RED_OUT" when using process image partitions

You use a separate process image partition for each priority class you require (OB1, OB 30 ... OB 38).

Hardware configuration and project engineering of the redundant I/O

Follow the steps below to use redundant I/O:

1. Insert all the modules you want to operate redundantly. Remember the following basic rules for project engineering.
2. Configure the module redundancy using HW Config in the object properties of the relevant module.

   Either browse for a partner module for each module, or accept the default settings

   In a centralized configuration: If the module is in slot X of the even-numbered rack, the module at the same slot position in the next odd-numbered rack is proposed.
   If the module is in slot X of the odd-numbered rack, the module at the same slot position in the previous even-numbered rack is proposed.

   Distributed configuration in a one-sided DP slave: If the module is inserted in slot X of the slave, the module at the same slot X of the slave at the same PROFIBUS address in the partner DP subsystem is proposed, provided the DP master system is redundant.

   Distributed configuration in a switched DP slave, stand-alone mode: If the module in the slave with a DP address is inserted in slot X, the module in the slave with the next PROFIBUS address at slot X is proposed.
3. Enter the remaining redundancy parameters for the input modules.

NOTICE
Always switch off power to the station or rack before you remove a redundant digital input module that does not support diagnostics functions and is not passivated. You might otherwise passivate the wrong module. This procedure is necessary, for example, when replacing the front connector of a redundant module. Redundant modules must be in the process image of the inputs or outputs. Redundant modules are always accessed using the process image. When using redundant modules, select the "Cycle/Clock Memory" tab from "HW Config -> Properties CPU 41x-H" and set the following: "OB 85 call on I/O access error > Only incoming and outgoing errors"

10.5.2 Signal modules for redundancy

Signal modules as redundant I/O

The signal modules listed below can be used as redundant I/O. Refer to the latest information about the use of modules available in the readme file and in the SIMATIC FAQs at http://www.siemens.com/automation/service&support under the keyword "Redundant I/O".

Table 10-2 Signal modules for redundancy

<table>
<tr><th>channel group (V5.x)</th><th>module (V3.x)</th><th>channel (V 4.x)</th><th>Module</th><th>Order number</th></tr>
<tr><td colspan="5">Central: Redundant DI dual-channel</td></tr>
<tr><td rowspan="2">X</td><td rowspan="2">X</td><td rowspan="2"></td><td>DI 16xDC 24V interrupt</td><td>6ES7421–7BH0x–0AB0</td></tr>
<tr><td colspan="2">Use with non-redundant encoder
• This module supports the "wire break" diagnostic function. To be able to implement this function, make sure that when using an encoder that evaluates with two inputs in parallel, a total current between 2.4 mA and 4.9 mA flows even at signal state "0".

You achieve this by installing a resistive load at the encoder. The value depends on the type of switch, and usually ranges between 6800 and 8200 ohms for contacts.

For Beros, calculate the resistive load based on this formula:
(30V / (4.9mA – I_R_Bero) < R < (20V / (2.4mA – I_R_Bero)</td></tr>
<tr><td>X</td><td>X</td><td></td><td>DI 32xDC 24V</td><td>6ES7421–1BL0x–0AA0</td></tr>
<tr><td>X</td><td>X</td><td></td><td>DI 32xUC 120V</td><td>6ES7421–1EL00–0AA0</td></tr>
<tr><td colspan="5">Distributed: Redundant DI dual-channel</td></tr>
<tr><td>X</td><td>X</td><td></td><td>DI16xDC 24 V, interrupt</td><td>6ES7321–7BH00–0AB0</td></tr>
<tr><td rowspan="2">X</td><td rowspan="2">X</td><td rowspan="2">X</td><td>DI16xDC 24 V</td><td>6ES7321–7BH01–0AB0</td></tr>
<tr><td colspan="2">In the event of an error on one channel, the entire group (2 channels) is passivated.
Use with non-redundant encoder
• This module supports the "wire break" diagnostic function. To be able to implement this function, make sure that when using an encoder that evaluates with two inputs in parallel, a total current between 2.4 mA and 4.9 mA flows even at signal state "0".

You achieve this by installing a resistive load at the encoder. The value depends on the type of switch, and usually ranges between 6800 and 8200 ohms for contacts.

For Beros, calculate the resistive load based on this formula:
(30V / (4.9mA – I_R_Bero) < R < (20V / (2.4mA – I_R_Bero)</td></tr>
<tr><td rowspan="2">X</td><td rowspan="2">X</td><td rowspan="2"></td><td>DI16xDC 24 V</td><td>6ES7321–1BH02–0AA0</td></tr>
<tr><td colspan="2">In some system states, an incorrect value of the first module could be read in briefly when the front connector of the second module is removed. This is prevented by using series diodes like those shown in figure F.1.</td></tr>
<tr><td rowspan="2">X</td><td rowspan="2">X</td><td rowspan="2"></td><td>DI32xDC 24 V</td><td>6ES7321–1BL00–0AA0</td></tr>
<tr><td colspan="2">In some system states, an incorrect value of the first module could be read in briefly when the front connector of the second module is removed. This is prevented by using series diodes like those shown in figure F.2.</td></tr>
</table>

channel group (V5.x)	module (V3.x)	channel (V 4.x)	Module	Order number
X	X		DI 8xAC 120/230V	6ES7321–1FF01–0AA0
X	X		DI 4xNamur [EEx ib]	6ES7321–7RD00–0AB0
			You cannot use the module for applications in hazardous areas in redundant mode. Use with non-redundant encoder • You can only connect 2-wire NAMUR encoders or contact encoders. • Equipotential bonding of the encoder circuit should always be at one point only (preferably encoder negative). • When selecting encoders, compare their properties with the specified input characteristics. Remember that this function must always guaranteed, regardless whether you are using one or two inputs. Example of valid values for NAMUR encoders: for "0" current > 0.2 mA; for "1" current > 4.2 mA.	
X	X		DI 16xNamur	6ES7321–7TH00–0AB0
			Use with non-redundant encoder • Equipotential bonding of the encoder circuit should always be at one point only (preferably encoder negative). • Operate the two redundant modules on a common load power supply. • When selecting encoders, compare their properties with the specified input characteristics. Remember that this function must always guaranteed, regardless whether you are using one or two inputs. Example of valid values for NAMUR encoders: for "0" current > 0.7 mA; for "1" current > 4.2 mA.	
X	X		DI 24xDC 24 V	6ES7326–1BK00–0AB0
			F module in standard operation	
X	X		DI 8xNAMUR [EEx ib]	6ES7326–1RF00–0AB0
			F module in standard operation	
Central: Redundant DO dual-channel				
X	X		DO 32xDC 24V/0.5A	6ES7422–7BL00–0AB0
			A clear evaluation of the diagnostics information "P short-circuit", "M short-circuit" and wire break is not possible. Deselect these individually in your configuration.	
X	X		DO 16xAC 120/230V/2A	6ES7422–1FH00–0AA0
Distributed: Redundant DO dual-channel				
X	X		DO8xDC 24 V/0.5 A	6ES7322–8BF00–0AB0
			A definite evaluation of the diagnostics information "P short-circuit" and wire break is not possible. Deselect these individually in your configuration. Since the module can only be operated in module-oriented redundancy, the diagnostic messages "M short-circuit" and " L+ - monitoring" cause a module error.	
X	X		DO8xDC 24 V/2 A	6ES7322–1BF01–0AA0
X	X		DO32xDC 24 V/0.5 A	6ES7322–1BL00–0AA0
X	X		DO8xAC 120/230 V/2 A	6ES7322–1FF01–0AA0
X	X		DO 4x24 V/10 mA [EEx ib]	6ES7322–5SD00–0AB0
			You cannot use the module for applications in hazardous areas in redundant mode.	
X	X		DO 4x24 V/10 mA [EEx ib]	6ES7322–5RD00–0AB0
			You cannot use the module for applications in hazardous areas in redundant mode.	

channel group (V5.x)	module (V3.x)	channel (V 4.x)	Module	Order number
X	X	X	DO 16xDC 24 V/0.5 A	6ES7322–8BH01–0AB0
			• The equipotential bonding of the load circuit should always be at one point only (preferably load minus). • Diagnostics of the channels is not possible.	
X	X	X	DO 10xDC 24 V/2 A as of product version 3	6ES7326–2BF01–0AB0
			The inputs and outputs must have the same address.	
Central: Redundant AI dual-channel				
X	X		AI 16x16Bit	6ES7431–7QH00–0AB0
			Use in voltage measurement • The "Wire break" diagnostics function in HW Config must not be activated either when operating the modules with measuring transducers or when thermocouples are connected. Use in indirect current measurement • Use a 50 ohm resistor (measuring range +/- 1V) or 250 ohm resistor (measuring range 1 - 5 V) to convert the current to a voltage, see figure 10-9. The tolerance of the resistor must be added on to the module error. Use in direct current measurement • Suitable Zener diode BZX85C6v2 or 1N4734A (6.2 V because of the 50 ohm input resistance) • Load capability of 4-wire measuring transducers: R_B > 325 ohms (worst-case: 1 input + 1 Zener diode at an S7 overshoot value 24 mA to $R_B = (R_E * I_{max} + U_{z\,max}) / I_{max}$) • Input voltage in the circuit when operating with a 2-wire measuring transducer: $U_{e-2w} < 8$ V (worst-case: 1 input + 1 Zener diode at an S7 overshoot value 24 mA to $U_{e-2w} = R_E * I_{max} + U_{z\,max}$) **Note:** The circuit shown in figure 10-10 works only with active (4-wire) measuring transducers or with passive (2-wire) measuring transducers with external power supply. Always configure the module channels for operation as "4-wire measuring transducer", and set the measuring range cube to position "C". It is not possible to power the measuring transducers via the module (2DMU).	

channel group (V5.x)	module (V3.x)	channel (V 4.x)	Module	Order number
Distributed: Redundant AI dual-channel				
X	X		AI8x12-bit	6ES7331–7KF02–0AB0
			Use in voltage measurement • The "Wire break" diagnostics function in HW Config must not be activated either when operating the modules with measuring transducers or when thermocouples are connected. Use for indirect current measurement • When establishing the measuring error please observe: The total input resistance in measuring ranges > 2.5 V can be reduced from a nominal 100 kilohms to 50 kilohms when operating two inputs in parallel. • The "Wire break" diagnostics function in HW Config must not be activated either when operating the modules with measuring transducers or when thermocouples are connected. • Use a 50 ohm resistor (measuring range +/- 1V) or 250 ohm resistor (measuring range 1 - 5 V) to convert the current to a voltage, see figure 10-9. The tolerance of the resistor must be added on to the module error. • This module is not suitable for direct current measurement. Use of redundant encoders: • You can use a redundant encoder with the following voltage settings: +/- 80 mV (only without wire break monitoring) +/- 250 mV (only without wire break monitoring) +/- 500 mV (wire break monitoring not configurable) +/- 1 V (wire break monitoring not configurable) +/- 2.5 V (wire break monitoring not configurable) +/- 5 V (wire break monitoring not configurable) +/- 10 V (wire break monitoring not configurable 1...5 V (wire break monitoring not configurable)	
X	X	X	AI 8x16-bit	6ES7331–7NF00–0AB0
			Use in voltage measurement • The "wire break" diagnostics function in HW Config must not be activated when operating the modules with measuring transducers. Use in indirect current measurement • When using indirect current measurement, ensure a reliable connection between the gauge resistances and the actual inputs, as, in the case of a wire break of individual cables, this connection cannot guarantee a secure wire break detection. • Use a 250 ohm resistor (measuring range 1 - 5 V) to convert the current to a voltage; see figure 10-9. Use in direct current measurement • Suitable Zener diodes: BZX85C8v2 or 1N4738A (8.2 V because of the 250 ohm input resistance) • Circuit-specific additional error: If one module fails, the other may suddenly show an additional error of approx. 0.1%. • Load capability of 4-wire measuring transducers: R_B > 610 ohms (worst-case: 1 input + 1 Zener diode at an S7 overshoot value 24 mA to R_B = (R_E * I_{max} + $U_{z\,max}$) / I_{max}) • Input voltage in the circuit when operating with a 2-wire measuring transducer: $U_{e\text{-}2w}$ < 15 V (worst-case: 1 input + 1 Zener diode at an S7 overshoot value 24 mA to $U_{e\text{-}2w}$ = R_E * I_{max} + $U_{z\,max}$)	

channel group (V5.x)	module (V3.x)	channel (V 4.x)	Module	Order number
X	X		AI 8x16-bit	6ES7331–7NF10–0AB0
			Use in voltage measurement • The "Wire break" diagnostics function in HW Config must not be activated either when operating the modules with measuring transducers or when thermocouples are connected. Use in indirect current measurement • Use a 250 ohm resistor (measuring range 1 - 5 V) to convert the current to a voltage; see figure 10-9. Use in direct current measurement • suitable Zener diodes: BZX85C8v2 or 1N4738A (8.2 V because of the 250 ohm input resistance) • Load capability of 4-wire measuring transducers: R_B > 610 ohms (worst-case: 1 input + 1 Zener diode at an S7 overshoot value 24 mA to $R_B = (R_E * I_{max} + U_{z\,max}) / I_{max}$) • Input voltage in the circuit when operating with a 2-wire measuring transducer: $U_{e\text{-}2w} < 15$ V (worst-case: 1 input + 1 Zener diode at an S7 overshoot value 24 mA to $U_{e\text{-}2w} = R_E * I_{max} + U_{z\,max}$)	
X			AI 6xTC 16Bit iso, 6ES7331-7PE10-0AB0	6ES7331-7PE10-0AB0
			Use in voltage measurement • The "wire break" diagnostics function in HW Config must not be activated when operating the modules with thermocouples. Use in indirect current measurement • Due to the maximum voltage range +/- 1 V, the indirect current measurement can be carried out exclusively via a 50 ohm resistor. A current that conforms to the system is only possible for the area +/- 20 mA.	
X	X		AI 4x15Bit [EEx ib]	6ES7331-7RD00-0AB0
			You cannot use the module for applications in hazardous areas in redundant mode. It is not suitable for indirect current measurement. Use in direct current measurement • Suitable Zener diode BZX85C6v2 or 1N4734A (6.2 V because of the 50 ohm input resistance) • Load capability of 4-wire measuring transducers: RB > 325 ohms Worst-case: 1 input + 1 Zener diode at an S7 overshoot value 24 mA to RB = (RE * $I_{max} + U_{z\,max}$) / I_{max} • Input voltage for 2-wire measuring transducers: Ue–2w < 8 V Worst-case: 1 input + 1 Zener diode at an S7 overshoot value 24 mA to Ue–2w = RE * $I_{max} + U_{z\,max}$ **Note:** You can only connect 2-wire measuring transducers with a 24 V external supply or 4-wire measuring transducers. The internal power supply for measuring transducers cannot be used in the circuit shown in figure 8-10 because this outputs only 13 V, and so in the worst case would supply only 5 V to the measuring transducer.	
X	X		AI 6x13-bit	6ES7336–1HE00–0AB0
			F module in standard operation	
X	X	X	AI 8x0/4...20mA HART	6ES7331–7TF01-0AB0
			See *Distributed I/O Device ET 200M; HART Analog Modules* manual	

channel group (V5.x)	module (V3.x)	channel (V 4.x)	Module	Order number
Distributed: Redundant AO dual-channel				
X	X		AO4x12-bit	6ES7332–5HD01–0AB0
X	X	X	AO8x12-bit	6ES7332–5HF00–0AB0
X	X		AO4x0/4...20 mA [EEx ib]	6ES7332–5RD00–0AB0
			You cannot use the module for applications in hazardous areas in redundant mode.	
X	X	X	AO 8x0/4...20mA HART	6ES7332–8TF01-0AB0
			See *Distributed I/O Device ET 200M; HART Analog Modules* manual	

NOTICE
You need to install the F Configuration Pack for F modules. The F Configuration Pack can be downloaded free of charge from the Internet. You can get it from Customer Support at: http://www.siemens.com/automation/service&support.

Quality levels in the redundant configuration of signal modules

The availability of modules in the case of an error depends on their diagnostics possibilities and the fine granularity of the channels.

Using digital input modules as redundant I/O

The following parameters are set to configure digital input modules for redundant operation:

- Discrepancy time (maximum permitted time in which the redundant input signals may differ). The configured discrepancy time must be a multiple of the update time of the process image and therefore also the basic conversion time of the channels.
  When there is still a discrepancy in the input values after the configured discrepancy time has expired, an error has occurred.
- Reaction to a discrepancy with the input values

First, the input signals of the paired redundant modules are checked for consistency. If the values match, the uniform value is written to the lower memory area of the process input image. If there is a discrepancy and it is the first, it is marked accordingly and the discrepancy time is started.

During the discrepancy time, the most recent matching (non-discrepant) value is written to the process image of the module with the lower address. This procedure is repeated until the values once again match within the discrepancy time or until the discrepancy time of a bit has expired.

If the discrepancy continues past the expiration of the configured discrepancy time, an error has occurred.

The defective side is localized according to the following strategy:

1. During the discrepancy time the most recent matching value is retained as the result.
2. Once the discrepancy time has expired the following error message is displayed:
   Error code 7960: "Redundant I/O: discrepancy time at digital input expired, error not yet localized". Passivation is not performed and no entry is made in the static error image. Until the next signal change occurs, the configured reaction is performed after the discrepancy time expires.
3. If another signal change now occurs, the module/channel in which the change occurred is the intact module/channel and the other module/channel is passivated.

NOTICE
The time that the system actually needs to determine a discrepancy depends on various factors: Bus delay times, cycle and call times in the user program, conversion times etc. Redundant input signals can therefore be different for longer than the configured discrepancy time.

Modules with diagnostic functions are also passivated by calling OB82.

Using redundant digital input modules with non-redundant encoders

With non-redundant encoders, you use digital input modules in a 1-out-of-2 configuration:

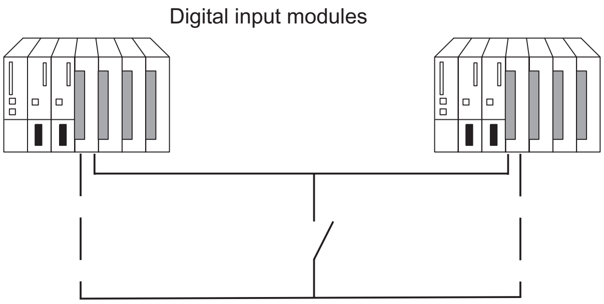


Figure 10-6 Fault-tolerant digital input module in 1-out-of-2 configuration with one encoder

The use of redundant digital input modules increases their availability.

Discrepancy analysis detects "Continuous 1" and "Continuous 0" errors of the digital input modules. A "Continuous 1" error means the value 1 is applied permanently at the input, a "Continuous 0" error means that the input is not energized. This can be caused, for example, by a short-circuit to L+ or M.

The current flow over the chassis ground connection between the modules and the encoder should be the minimum possible.

When connecting an encoder to several digital input modules, the redundant modules must operate at the same reference potential.

If you want to replace a module during operation and are not using redundant encoders, you will need to use decoupling diodes.

You will find connection examples in Appendix Connection examples for redundant I/Os (Page 375).

Note

Remember that the proximity switches (Beros) must provide the current for the channels of both digital input modules. The technical data of the respective modules however specify only the required current per input.

Using redundant digital input modules with redundant encoders

With redundant encoders you use digital input modules in a 1-out-of-2 configuration:

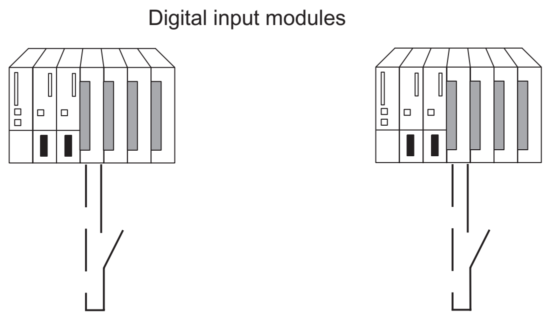


Figure 10-7 Fault-tolerant digital input modules in 1-out-of-2 configuration with two encoders

The use of redundant encoders also increases their availability. Discrepancy analysis detects all errors, except for the failure of a non-redundant load voltage supply. You can enhance availability by installing redundant load power supplies.

You will find connection examples in Appendix Connection examples for redundant I/Os (Page 375).

Redundant digital output modules

Redundant control of an actuator can be achieved by connecting two outputs of two digital output modules or fail-safe digital output modules in parallel (1-out-of-2 configuration)

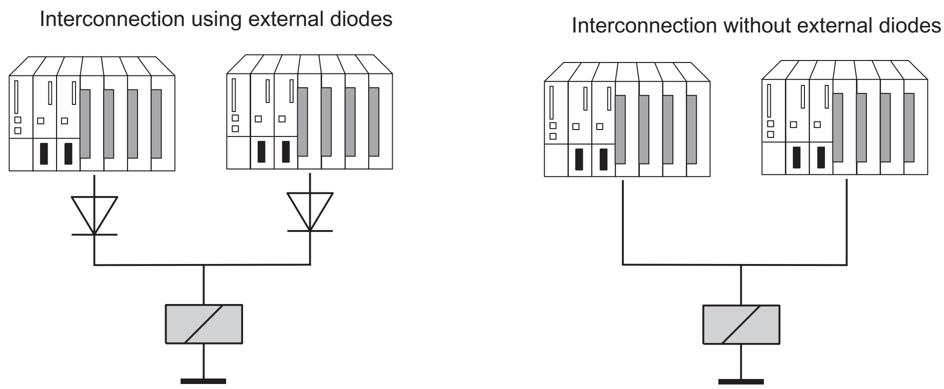


Figure 10-8 Fault-tolerant digital output modules in 1-out-of-2 configuration

The digital output modules must be connected to a common load voltage supply.

You will find connection examples in Appendix Connection examples for redundant I/Os (Page 375).

Interconnection using external diodes <-> without external diodes

The table below lists the redundant digital output modules you should interconnect using external diodes:

Table 10-3 Interconnecting digital output modules with/without diodes

Module	with diodes	without diodes
6ES7422–7BL00–0AB0	X	-
6ES7422–1FH00–0AA0	-	X
6ES7326–2BF01–0AB0	X	X
6ES7322–1BL00–0AA0	X	-
6ES7322–1BF01–0AA0	X	-
6ES7322–8BF00–0AB0	X	X
6ES7322–1FF01–0AA0	-	X
6ES7322–8BH01–0AB0	-	X
6ES7322–5RD00–0AB0	X	-
6ES7322–5SD00–0AB0	X	-

Information on wiring the diode circuit

- Suitable diodes are, for example, those of the series 1N4003 ... 1N4007, or other diodes with U_r >=200 V and I_F >= 1 A.
- It is advisable to separate the chassis ground of the module and load ground. There must be equipotential bonding between both.

Using analog input modules as redundant I/O

You specified settings for the following parameters when you configured the analog input modules for redundant mode:

- Tolerance window (configured as a percentage of the end value of the measuring range)
  Two analog values are considered equal if they are within the tolerance window.
- Discrepancy time (maximum permitted time in which the redundant input signal can be outside the tolerance window). The configured discrepancy time must be a multiple of the update time of the process image and therefore also the basic conversion time of the channels.
  An error is generated when there is an input value discrepancy after the configured discrepancy time has expired.
  If you connect identical sensors to both analog input modules, the default value for the discrepancy time is usually sufficient. If you connect different sensors, in particular temperature sensors, you will have to increase the discrepancy time.
- Applied value
  The applied value represents the value of the two analog input values that is entered in the user program.

The system verifies that the two read-in analog values are within the configured tolerance window. If they are, the applied value is written to the lower data memory area of the process input image. If there is a discrepancy and it is the first, it is marked accordingly and the discrepancy time is started.

When the discrepancy time is running, the most recent valid value is written to the process image of the module with the lower address and made available to the current process. If the discrepancy time expires, the module/channel with the configured standard value is declared as valid and the other module/channel is passivated. If the maximum value from both modules is configured as the standard value, this value is then taken for further program execution and the other module/channel is passivated. If the minimum value is configured, this module/channel supplies the data to the process and the module with the maximum value is passivated. In any case, the passivated modules/channels are entered in the diagnostic buffer.

If the discrepancy is eliminated within the discrepancy time, analysis of the redundant input signals is still carried out.

NOTICE
The time that the system actually needs to determine a discrepancy depends on various factors: Bus delay times, cycle and call times in the user program, conversion times etc. Redundant input signals can therefore be different for longer than the configured discrepancy time.

Note

There is no discrepancy analysis when a channel reports an overflow with 16#7FFF or an underflow with 16#8000. The relevant module/channel is passivated immediately.

You should therefore disable all unused inputs in HW Config using the "Measuring type" parameter.

Redundant analog input modules with non-redundant encoders

With non-redundant encoders, analog input modules are used in a 1-out-of-2 configuration:

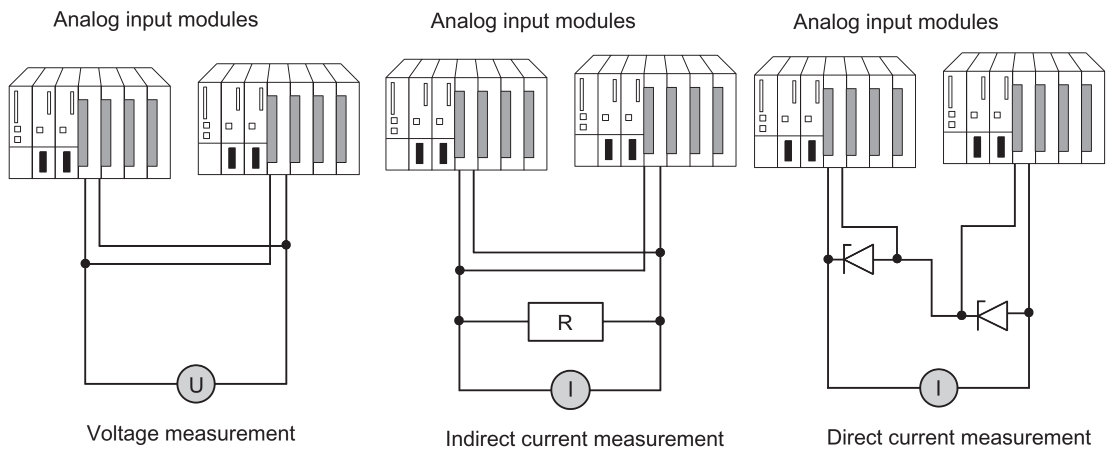


Figure 10-9 Fault-tolerant analog input modules in 1-out-of-2 configuration with one encoder

Remember the following when connecting an encoder to multiple analog input modules:

- Connect connect the analog input modules in parallel for voltage encoders (left in illustration).
- You can convert a current into voltage using an external load to use voltage analog input modules connected in parallel (center in the illustration.)
- 2-wire measuring transducers are powered externally to allow you to repair the module online.

The redundancy of the fail-safe analog input modules enhances their availability.

You will find connection examples in Appendix Connection examples for redundant I/Os (Page 375).

Redundant analog input modules for indirect current measurement

The following applies to the wiring of analog input modules:

- Suitable encoders for this circuit are active measuring transducers with voltage output and thermocouples.
- The "Wire break" diagnostics function in HW Config must not be activated either when operating the modules with measuring transducers or when thermocouples are connected.
- Suitable encoder types are active 4-wire and passive 2-wire measuring transducers with output ranges +/-20 mA, 0...20 mA and 4...20 mA. 2-wire measuring transducers are powered by an external auxiliary voltage.
- Criteria for the selection of resistance and input voltage range are the measurement accuracy, number format, maximum resolution and possible diagnostics.
- In addition to the options listed, other input resistance and voltage combinations according to Ohm's law are also possible. Note, however, that such combinations may lead to the loss of the number format, diagnostics function and resolution. The measurement error also depends largely on the size of the measuring resistor of certain modules.
- Use a measurement resistance with a tolerance of +/- 0.1% and TC 15 ppm.

Additional conditions for specific modules

AI 8x12-bit 6ES7331–7K..02–0AB0

- Use a 50 ohm or 250 ohm resistance to convert the current to a voltage:

Resistance	50 ohms	250 ohms	
Current measuring range	+/-20 mA	+/-20 mA *)	4...20 mA
Input range to be set	+/-1 V	+/-5 V	1...5 V
Measuring range cube position	"A"	"B"	
Resolution	12-bit+sign	12-bit+sign	12-bit
S7 number format	x	x	
Circuit-specific measuring error - 2 parallel inputs - 1 input	- -	0,5% 0,25%	
"Wire break" diagnostics	-	-	x *)
Load for 4-wire measuring transducers	50 ohms	250 ohms	
Input voltage for 2-wire measuring transducers	> 1.2 V	> 6 V	
*) The AI 8x12-bit outputs diagnostic interrupt and measured value "7FFF" in the event of wire break.			

The listed measuring error results solely from the interconnection of one or two voltage inputs with a measuring resistor. Allowance has not been made here for the error tolerance, or for the basic/operational error limits of the modules.

The measuring error for one or two inputs shows the difference in the measurement result depending on whether two inputs or, in case of error, only one input acquires the current of the measuring transducer.

AI 8x16-bit 6ES7331–7NF00–0AB0

- Use a 250 ohm resistor to convert the current to a voltage:

Resistance	250 ohms *)	
Current measuring range	+/-20 mA	4...20 mA
Input range to be set	+/-5 V	1...5 V
Resolution	15-bit+sign	15-bit
S7 number format	x	
Circuit-specific Measuring error - 2 parallel inputs - 1 input	- -	
"Wire break" diagnostics	-	x
Load for 4-wire measuring transducers	250 ohms	
Input voltage for 2-wire measuring transducers	> 6 V	
*) It may be possible to use the freely connectable internal 250 ohm resistors of the module		

AI 16x16-bit 6ES7431–7QH00–0AB0

- Use a 50 ohm or 250 ohm resistance to convert the current to a voltage:

Resistance	50 ohms	250 ohms	
Current measuring range	+/-20 mA	+/-20 mA	4...20 mA
Input range to be configured	+/-1 V	+/-5 V	1...5 V
Measuring range cube position	"A"	"A"	
Resolution	15-bit + sign	15-bit+sign	15-bit
S7 number format	x	x	
Circuit-specific Measuring error 1) - 2 parallel inputs - 1 input	- -	- -	
"Wire break" diagnostics	-	-	x
Load for 4-wire measuring transducers	50 ohms	250 ohms	
Input voltage for 2-wire measuring transducers	> 1.2 V	> 6 V	

Redundant analog input modules for direct current measurement

Requirements for wiring analog input modules according to Figure 8-10:

- Suitable encoder types are active 4-wire and passive 2-wire measuring transducers with output ranges +/-20 mA, 0...20 mA and 4...20 mA. 2-wire measuring transducers are powered by an external auxiliary voltage.
- The "wire break" diagnostics function supports only the 4...20 mA input range. All other unipolar or bipolar ranges are excluded in this case.
- Suitable diodes include the BZX85 or 1N47..A series (Zener diodes 1.3 W) with the voltages specified for the modules. When selecting other elements, make sure that the reverse current is as low as possible.
- A fundamental measuring error results from this type of circuit and the specified diodes, due to the maximum reverse current of 1 μA. In the 20 mA range, and at a resolution of 16 bits, this leads to an error of < 2 bits. Individual analog inputs in the circuit above lead to an additional error, which may be listed in the constraints. The errors specified in the manual must be added to these errors for all modules.
- The 4-wire measuring transducers used must be capable of driving the load resistance resulting from the circuit above. You will find details in the technical specifications of the individual modules.
- When connecting up 2-wire measuring transducers, note that the Zener diode circuit weighs heavily in the power budget of the measuring transducer. The required input voltages are therefore included in the technical specifications of the individual modules. Together with the inherent supply specified on the measuring transducer data sheet, the minimum supply voltage is calculated to $L+ > U_{e-2w} + U_{EV-MU}$

Redundant analog input modules with redundant encoders

With double-redundant encoders, it is better to use fail-safe analog input modules in a 1-out-of-2 structure:

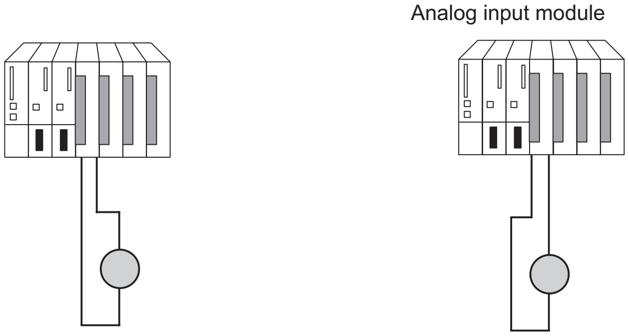


Figure 10-10 Fault-tolerant analog input modules in 1-out-of-2 structure with two encoders

The use of redundant encoders also increases their availability.

A discrepancy analysis also detects external errors, except for the failure of a non-redundant load voltage supply.

You will find connection examples in Appendix Connection examples for redundant I/Os (Page 375).

The general comments made at the beginning of this documentation apply.

Redundant encoders <-> non-redundant encoders

The table below shows you which analog input modules you can operate in redundant mode with redundant or non-redundant encoders:

Table 10-4 Analog input modules and encoders

Module	Redundant encoders	Non-redundant encoders
6ES7431–7QH00–0AB0	X	X
6ES7336–1HE00–0AB0	X	-
6ES7331–7KF02–0AB0	X	X
6ES7331–7NF00–0AB0	X	X
6ES7331–7RD00–0AB0	X	X

Redundant analog output modules

You implement fault-tolerant control of a final control element by wiring two outputs of two analog output modules in parallel (1-out-of-2 structure).

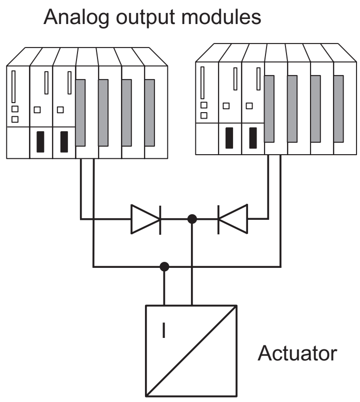


Figure 10-11 Fault-tolerant analog output modules in 1-out-of-2 configuration

The following applies to the wiring of analog output modules:

- Wire the ground connections in a star structure to avoid output errors (limited common-mode suppression of the analog output module).

Information on wiring the diode circuit

- Suitable diodes are, for example, those of the series 1N4003 ... 1N4007, or other diodes with U_r >=200 V and I_F >= 1 A.
- It is advisable to separate the module ground and the load ground. Both must be wired to different potential rails. There must be equipotential bonding between both

Analog output signals

Only analog output modules with current outputs (0 to 20 mA, 4 to 20 mA) can be operated redundantly.

The output value is divided by 2, and each of the two modules outputs half. If one of the modules fails, the failure is detected and the remaining module outputs the full value. As a result, the surge at the output module in the event of an error is not as high.

Note

The output value drops briefly to half, and after the reaction in the program, it then recovers to the proper value.

In the case of passivation or a CPU STOP, redundant analog outputs output a minimum current of approximately 120 µA per module, meaning a total current of approximately 240 µA. Allowing for the tolerance, this means that the output value is always positive. A configured substitute value of 0 mA will produce at least these output values. In redundant mode, in the event of a CPU STOP the current outputs are automatically configured to "off current and off voltage".

NOTICE
If there are two redundant analog output modules and an error occurs on the second module, as long as the first module is still passivated only half the current value is output on the faulty channels - even though both modules are passivated - until at least one of the two modules has been repaired.

Depassivation of modules

Passivated modules are depassivated by the following events:

- When the fault-tolerant system starts up
- When the H system changes over to "redundant" state
- After system modifications in operation
- If you call FC 451 "RED_DEPA" and at least one redundant channel or module is passivated.

The depassivation is executed in FB 450 "RED IN" after one of these events has occurred. Completion of the depassivation of all modules is logged in the diagnostic buffer.

Note

When a redundant module is assigned a process image partition and the corresponding OB is not available on the CPU, the complete passivation may take approximately 1 minute.

10.5.3 Evaluating the passivation status

Procedure

First, determine the passivation status by evaluating the status byte in the status/control word "FB_RED_IN.STATUS_CONTROL_W" . If you then see that one or more modules have been passivated, evaluate the status of the respective module pairs in MODUL_STATUS_WORD.

Evaluating the passivation status using the status byte

The status word "FB_RED_IN.STATUS_CONTROL_W" is located in the instance DB of FB 450 "RED_IN". The status byte returns information on the status of the redundant I/Os. The assignment of the status byte is described in the online help for the respective block library.

Evaluating the passivation status of individual module pairs by means of MODUL_STATUS_WORD

MODUL_STATUS_WORD is an output parameter of FB 453 and can be interconnected accordingly. It returns information on the status of individual module pairs.

The assignment of the MODUL_STATUS_WORD status byte is described in the online help for the respective block library.

10.6 Other options for connecting redundant I/Os

Redundant I/O at user level

If you cannot use the redundant I/O supported by your system (section Connecting redundant I/Os (Page 138)), for example because the relevant module may not be listed among the supported components, you can implement the use of redundant I/O at the user level.

Configurations

The following redundant I/O configurations are supported:

1. Redundant configuration with one-sided central and/or distributed I/O.

   For this, in each case one signal module is inserted into each of the CPU 0 and CPU 1 subsystems.

2. Redundant configuration with switched I/O

   One signal module is inserted into each of two ET 200M distributed I/O devices with active backplane bus.

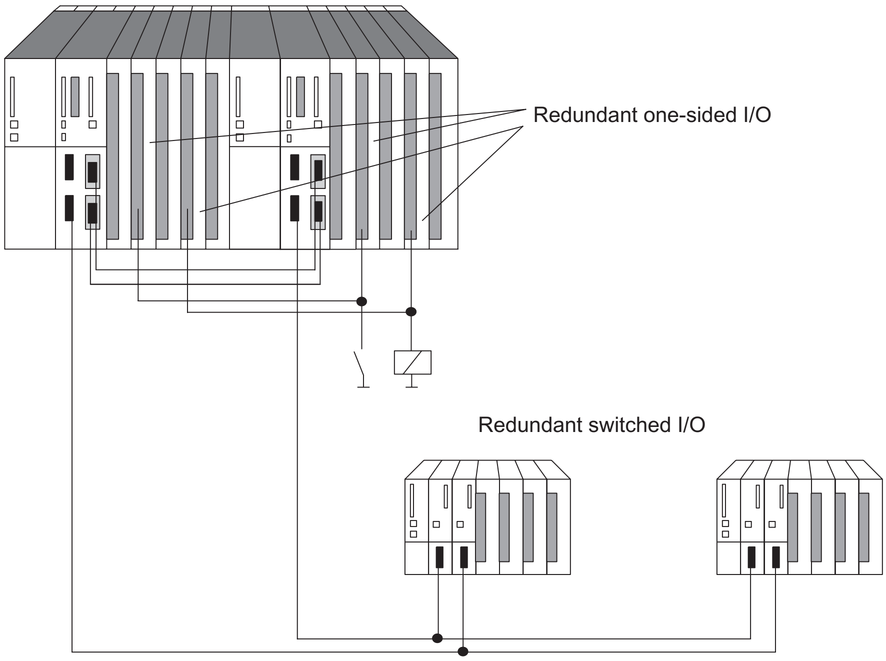


Figure 10-12 Redundant one-sided and switched I/O

NOTICE
When using redundant I/O, you may need to add an overhead to the calculated monitoring times; see section Determining the monitoring times (Page 118).

Hardware configuration and project engineering of the redundant I/O

Strategy recommended for use of redundant I/O:

1. Use the I/O as follows:
   - in a one-sided configuration, in each case one signal module per subsystem
   - in a switched configuration, in each case one signal module in each of two ET 200M distributed I/O devices.
2. Wire the I/O in such a way that it can be addressed by both subsystems.
3. Configure the signal modules so that they have different logical addresses.

> **NOTICE**
>
> It is not advisable to configure the input and output modules with the same logical addresses. Otherwise, in addition to the logical address, you will also need to query the type (input or output) of the defective module in OB 122.
>
> The user program also has to update the process image for redundant one-sided output modules when the system is in single mode (direct access, for example). If you use process image partitions, the user program must update them (SFC27 "UPDAT_PO") in OB 72 (recovery of redundancy). The system would otherwise initialize the single-channel one-sided output modules of the standby CPU with the old values after the system change to redundant mode.

Redundant I/O in the user program

The sample program below shows the use of two redundant digital input modules:

- Module A in rack 0 with logical base address 8 and
- module B in rack 1 with logical base address 12.

One of the two modules is read in OB1 by direct access. For the following it is generally assumed that the module in question is A (value of variable MODA is TRUE). If no error occurred, processing continues with the value read.

If an I/O access error has occurred, module B is read by direct access ("retry" in OB1). If no error occurred, processing of module B continues with the value read. However, if an error has also occurred here, both modules are currently defective, and operation continues with a substitute value.

The sample program is based on the fact that, following an access error on module A or its replacement, module B is always processed first in OB1. Module A is not processed first again in OB1 until an access error occurs on module B.

NOTICE
The MODA and IOAE_BIT variables must also be valid outside OB1 and OB122. The ATTEMPT2 variable, however, is used only in OB1.

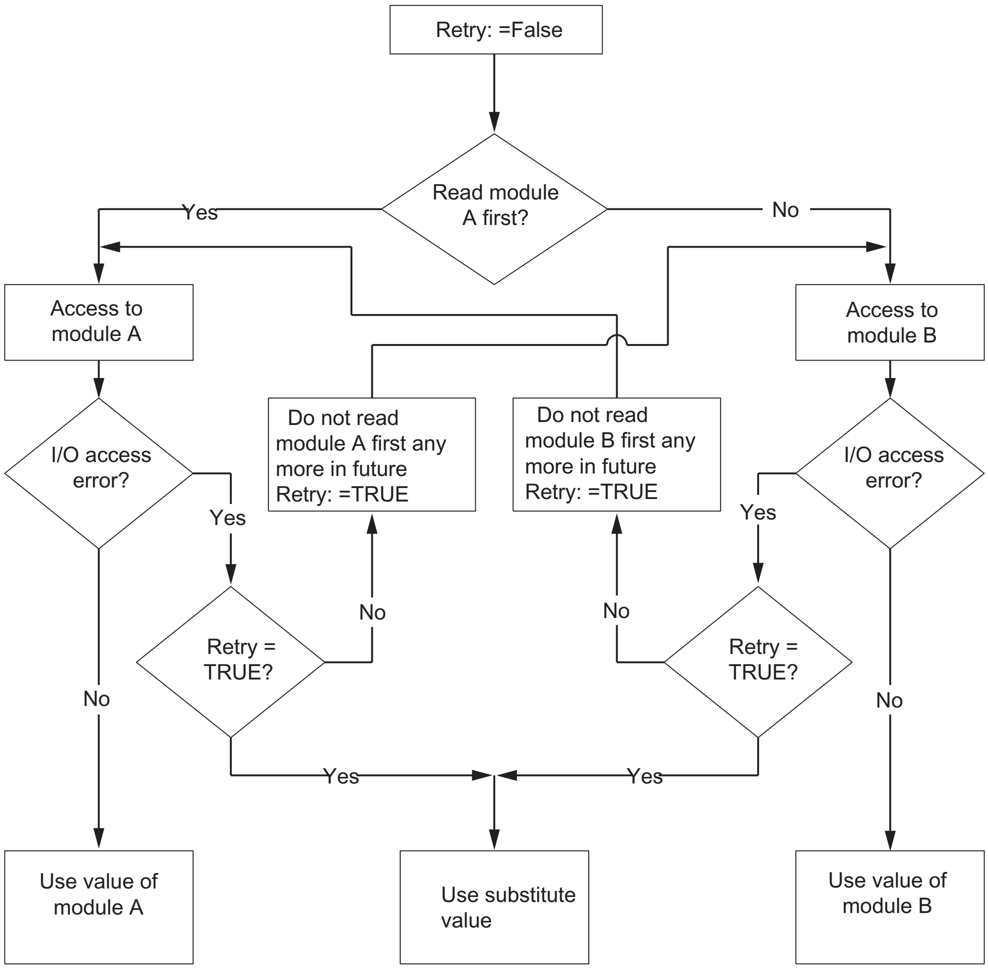


Figure 10-13 Flow chart for OB1

Example in STL

The required elements of the user program (OB1, OB 122) are listed below.

Table 10-5 Example of redundant I/O, OB1 part

STL	Description
NOP 0;	
SET;	
R ATTEMPT2;	//Initialization
A MODA;	//Read module A first?
JCN CMOB;	//If not, continue with module B
CMOA: SET;	
R IOAE_BIT;	//Delete IOAE bit
L PID 8;	//Read from CPU 0
A IOAE_BIT;	//Was IOAE detected in OB 122?
JCN IOOK;	//If not, process access OK
A ATTEMPT2;	//Was this access the second attempt?
JC CMO0;	//If yes, use substitute value
SET;	
R MODA;	//Do not read module A first any more //in future
S ATTEMPT2;	
CMOB: SET;	
R IOAE_BIT;	//Delete IOAE bit
L PID 12;	//Read from CPU 1
A IOAE_BIT;	//Was IOAE detected in OB 122?
JCN IOOK;	//If not, process access OK
A ATTEMPT2;	//Was this access the second attempt?
JC CMO0;	//If yes, use substitute value
SET;	
S MODA;	//Read module A first again in future
S ATTEMPT2;	
JU CMOA;	
CMO0: L SUBS;	//Substitute value
IOOK:	//The value to be used is in ACCU1

Table 10-6 Example of redundant I/O, OB 122 part

STL	Description
	// Does module A cause IOAE?
L OB122_MEM_ADDR;	//Relevant logical base address
L W#16#8;	
== I;	//Module A?
JCN M01;	//If not, continue with M01
	//IOAE during access to module A
SET;	
= IOAE_BIT;	//Set IOAE bit
JU CONT;	
	// Does module B cause a IOAE?
M01: NOP 0;	
L OB122_MEM_ADDR;	//Relevant logical base address
L W#16#C;	
== I;	//Module B?
JCN CONT;	//If not, continue with CONT
	//IOAE during access to module B
SET;	
= IOAE_BIT;	//Set IOAE bit
CONT: NOP 0;	

Monitoring times in link-up and update

NOTICE

If you have made I/O modules redundant and have taken account of this in your program, you may need to add an overhead to the calculated monitoring times so that no bumps occur at output modules (in HW Config -> Properties CPU -> H Parameter).

An overhead is only required if you operate modules from the following table as redundant.

Table 10-7 For the monitoring times I/O used redundantly

Module type	Overhead in ms
ET200M: Standard output modules	2
ET200M: HART output modules	10
ET200M: F output modules	50
ET200L–SC with analog outputs	≤ 80
ET200S with analog outputs or technology modules	≤ 20

Follow the steps below:

- Calculate the overhead from the table. If you have used several module types from the table redundantly, apply the largest overhead.
- Add this to all the monitoring times calculated so far.

11 Communication

11.1 Communication

This section provides an introduction to communications with fault-tolerant systems and their specific characteristics.

It sets out the basic concepts, the bus systems you can use for fault-tolerant communications, and the available types of connection.

It contains information on communication functions using fault-tolerant and standard connections, and explains how to configure and program them.

- You will also find examples of communication over fault-tolerant S7 connections and learn about the advantages it offers.
- By way of comparison, you will learn how communication takes place over S7 connections and how you can also communicate in redundant mode by means of S7 connections.

11.2 Fundamentals and basic concepts

Overview

Rising demands on the availability of an overall system make it essential to improve the fail-safety of communication systems, including implementation of redundant communication.

You will find below an overview of the fundamentals and basic concepts which you ought to know with regard to using fault-tolerant communications.

Redundant communication system

The availability of the communication system can be enhanced by redundancy of the media, duplication of component units, or duplication of all bus components.

On failure of a component, the various monitoring and synchronization mechanisms ensure that the communication functions are taken over by the standby components while the system stays in operation.

A redundant communication system is essential if you want to use fault-tolerant S7 connections.

Fault-tolerant communication

Fault-tolerant communication is the deployment of S7 communication SFBs over fault-tolerant S7 connections.

Fault-tolerant S7 connections are only possible when using redundant communication systems.

Redundancy nodes

Redundancy nodes represent the fail-safety of communication between two fault-tolerant systems. A system with multi-channel components is represented by redundancy nodes. Redundancy nodes are independent when the failure of a component within the node does not result in any reliability impairment in other nodes.

Even with fault-tolerant communication, only single errors/faults can be tolerated. If more than one error/fault occurs between communication endpoints, communication can no longer be guaranteed.

Connection (S7 connection)

A connection represents the logical assignment of two communication partners executing a communication service. Every connection has two end points containing the information required for addressing the communication partner as well as other attributes for establishing the connection.

An S7 connection is the communication link between two standard CPUs or from one standard CPU to a CPU in a fault-tolerant system.

In contrast to a fault-tolerant S7 connection, which contains at least two partial connections, an S7 connection actually consists of just one connection. If that connection fails, communication is terminated.

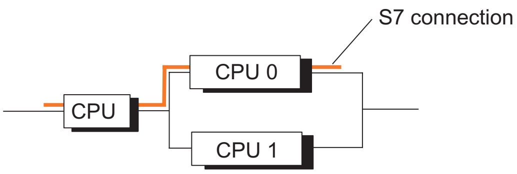


Figure 11-1 Example of an S7 connection

Note

Generally speaking, "connection" in this manual means a "configured S7 connection". For other types of connection please refer to the *SIMATIC NET NCM S7 for PROFIBUS* and *SIMATIC NET NCM S7 for Industrial Ethernet* manuals.

Fault-tolerant S7 connections

The requirement for higher availability with communication components (for example CPs and buses) means that redundant communication connections are necessary between the systems involved.

Unlike an S7 connection, a fault-tolerant S7 connection consists of at least two underlying subconnections. From a user program, configuration and connection diagnostics perspective, the fault-tolerant S7 connection with its underlying subconnections is represented by exactly one ID (just like a standard S7 connection). Depending on the configuration, it can consist of up to four subconnections, of which two are always established (active) to maintain communication in the event of an error. The number of subconnections depends on the possible alternative paths (see figure below) and is identified automatically.

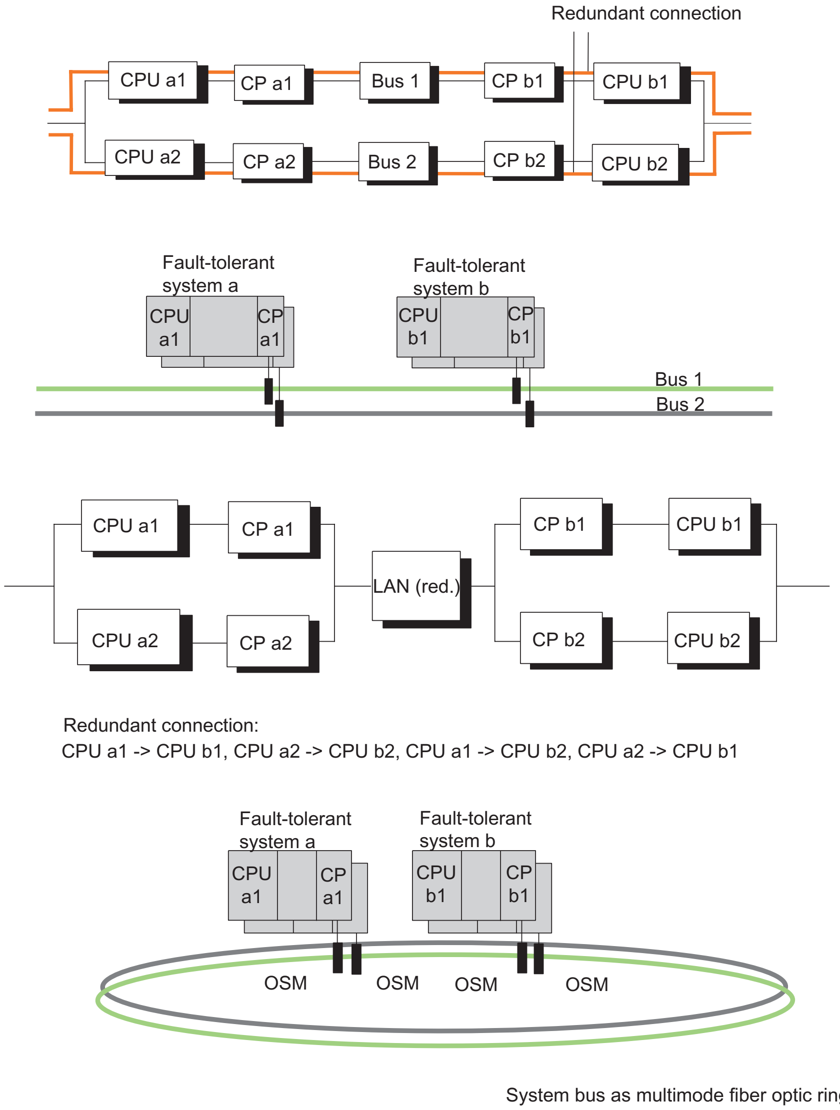


Figure 11-2 Example of how number of resulting subconnections depends on the configuration

If the active subconnection fails, the already established second subconnection automatically takes over communication.

Resource requirements of fault-tolerant S7 connections

The fault-tolerant CPU supports the operation of 62/30/14 (see the technical specifications) fault-tolerant S7 connections. On the CP each subconnection requires a connection resource.

NOTICE
If you have configured several fault-tolerant S7 connections for a fault-tolerant station, establishing them may take a considerable time. If the configured maximum communication delay is set too short, link-up and updating is aborted and the redundant system state is no longer reached (see section Time monitoring (Page 114)).

11.3 Usable networks

Your choice of the physical transmission medium depends on the required expansion, targeted fault tolerance and transmission rate. The following bus systems are used for communication with fault-tolerant systems:

- Industrial Ethernet (fiber-optic cable, triaxial or twisted-pair copper cable)
- PROFIBUS (fiber-optic cable or copper cable)

For further information on suitable networks, refer to the *Communication with SIMATIC*", *"Industrial Twisted Pair Networks* and *"PROFIBUS Networks* manuals.

11.4 Usable communication services

The following services can be used:

- S7 communication using fault-tolerant S7 connections via PROFIBUS and Industrial Ethernet Fault-tolerant S7 connections are possible only between SIMATIC S7 stations. Fault-tolerant communication is possible over Industrial Ethernet only with the ISO protocol.
- S7 communications using S7 connections via MPI, PROFIBUS and Industrial Ethernet
- Standard communication (e.g. FMS) via PROFIBUS
- S5-compatible communication (e.g. SEND and RECEIVE blocks) via PROFIBUS and Industrial Ethernet

The following are not supported:

- S7 basic communication
- Global data communication
- Open communication via Industrial Ethernet

11.5 Communications via fault-tolerant S7 connections

Availability of communicating systems

Fault-tolerant communication expands the overall SIMATIC system by additional, redundant communication components, such as CPs and bus cables. To illustrate the actual availability of communicating systems when using an optical or electrical network, a description is given below of the possibilities for communication redundancy.

Requirements

The essential requirement for the configuration of fault-tolerant connections with STEP 7 is a configured hardware installation.

The hardware configuration in both subsystems of the redundant systems **must** be identical. This applies in particular to the slots.

Depending on the network you are using, CPs can be used for fault-tolerant and fail-safe communication, see Appendix Function modules and communication processors supported by the S7-400H (Page 373)
Only Industrial Ethernet with the ISO protocol is supported.

To be able to use fault-tolerant S7 connections between a fault-tolerant system and a PC, you must install the "S7-REDCONNECT" software package on the PC. Please refer to the Product Information on "S7-REDCONNECT" to learn more about the CPs you can use at the PC end.

Configuration

The availability of the system, including the communication, is set during configuration. Refer to the STEP 7 documentation to find out how to configure connections.

Only S7 communication is used for fault-tolerant S7 connections. To set this up, open the "New Connection" dialog box, then select "S7 Connection Fault-Tolerant" as the type.

The number of required redundant connections is determined by STEP 7 as a function of the redundancy nodes. Up to four redundant connections will be generated, if supported by the network. Higher redundancy can not be achieved even by using more CPs.

In the "Properties - Connection" dialog box you can also modify specific properties of a fault-tolerant connection if necessary. When using more than one CP, you can also route the connections in this dialog box. This may be practical, because by default all connections are routed initially through the first CP. If all the connections are busy there, any further connections are routed via the second CP, etc.

Programming

Fault-tolerant communication can be deployed on the fault-tolerant CPU and is implemented by means of S7 communication.

This is possible only within an S7 project/multiproject.

Fault-tolerant communication is programmed in STEP 7 by means of communication SFBs. Those blocks can be used to transfer data on subnets (Industrial Ethernet, PROFIBUS). The standard communication SFBs integrated into the operating system offer you the option of acknowledged data transfer. In addition to data transfer, you can also use other communication functions for controlling and monitoring the communication partner.

User programs written for standard communication can also be run for fault-tolerant communication without modification. Cable and connection redundancy has no effect on the user program.

Note

For information on programming the communication, refer to the STEP 7 documentation (e.g. *Programming with STEP 7*).

The START and STOP communication functions act on exactly one CPU or on all CPUs of the fault-tolerant system (for more details refer to the *System Software for S7-300/400, System and Standard Functions* reference manual) reference manual.

Any disruption of subconnections while communication requests are active over fault-tolerant S7 connections leads to extended delay times.

NOTICE
Downloading connection configuration during operation
If you download a connection configuration during operation, any established connections could be aborted.

11.5.1 Communication between fault-tolerant systems

Availability

The easiest way to enhance availability between linked systems is to implement a redundant system bus, using a multimode (duplex) fiber-optic ring or a dual electrical bus system. In this, the connected nodes may consist of simple standard components.

Availability can best be enhanced using a multimode fiber-optic ring topology. If the one of the multimode fiber-optic cables breaks, communication between the systems involved is maintained. The systems then communicate as if they were connected to a bus system (line). A ring topology basically contains two redundant components, and so automatically forms a 1-of-2 redundancy node. A fiber-optic network can be set up as a line or star topology. However, the line topology does not offer cable redundancy.

If one electrical cable segment fails, communication between the partner systems is also upheld (1-of-2 redundancy).

The examples below illustrate the differences between the two variants.

Note

The number of connection resources required on the CPs depends on the network you are using.

If you implement an optical two-fiber ring (see figure below), two connection resources are required per CP. In contrast, only one connection resource is required per CP if a double electrical network (see figure after next) is used.

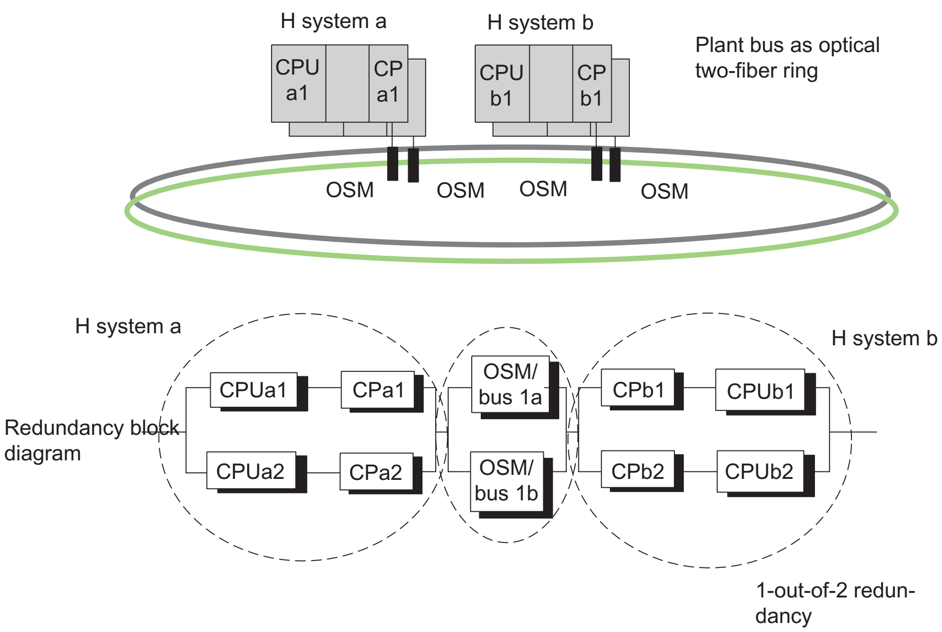


Figure 11-3 Example of redundancy with fault-tolerant system and redundant ring

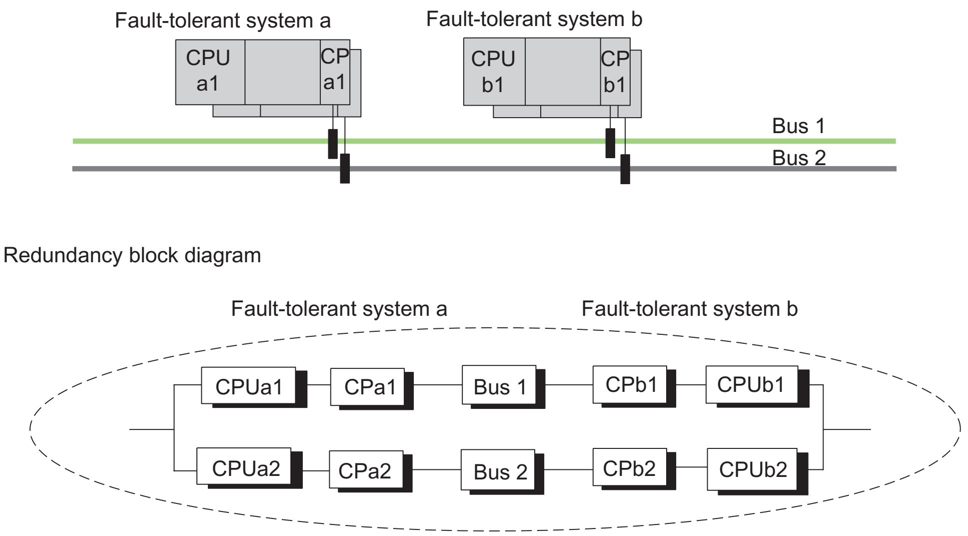


Figure 11-4 Example of redundancy with fault-tolerant system and redundant bus system

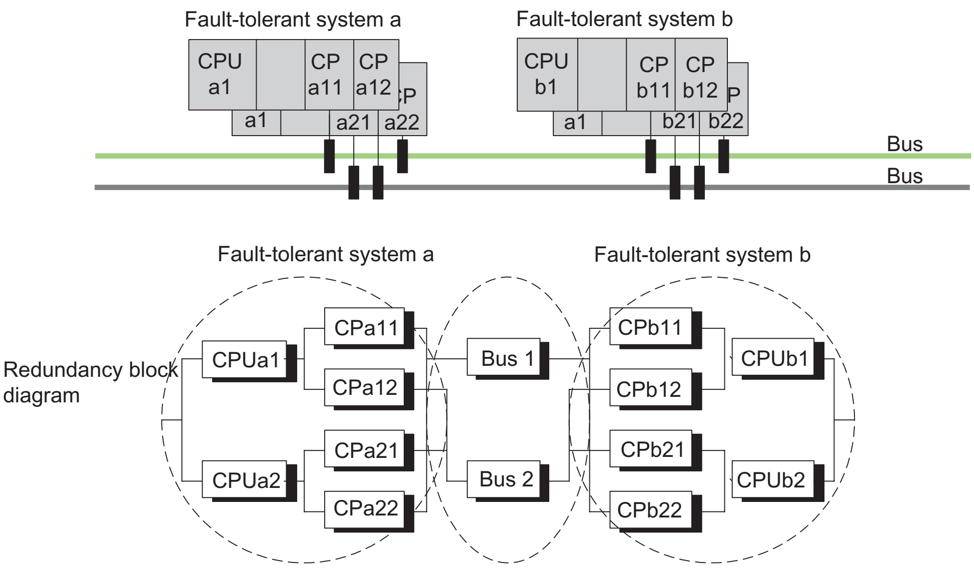


Figure 11-5 Example of fault-tolerant system with additional CP redundancy

Reaction to failure

If a two-fiber ring is used, only a double error within a fault-tolerant system (e.g. CPUa1 and CPa2 in one system) leads to total failure of communication between the systems involved (see first figure).

If a double error (e.g. CPUa1 and CPb2) occurs in the first case of a redundant electrical bus system (see second figure), this results in a total failure of communication between the systems involved.

In the case of a redundant electrical bus system with CP redundancy (see third figure), only a double error within a fault-tolerant system (e.g. CPUa1 and CPUa2) or a triple error (e.g. CPUa1, CPa22 and bus2) will result in a total failure of communication between the systems involved.

Fault-tolerant S7 connections

Any disruption of subconnections while communication requests are active over fault-tolerant S7 connections leads to extended delay times.

11.5.2 Communication between fault-tolerant systems and a fault-tolerant CPU

Availability

Availability can be enhanced by using a redundant system bus and by using a fault-tolerant CPU on a standard system.

If the communication partner is a fault-tolerant CPU, redundant connections can also be configured, in contrast to systems with a 416 CPU for example.

Note

Fault-tolerant connections use two connection resources on CP b1 for the redundant connections. One connection resource each is occupied on CP a1 and CP a2 respectively. In this case, the use of further CPs in the standard system only serves to increase the resources.

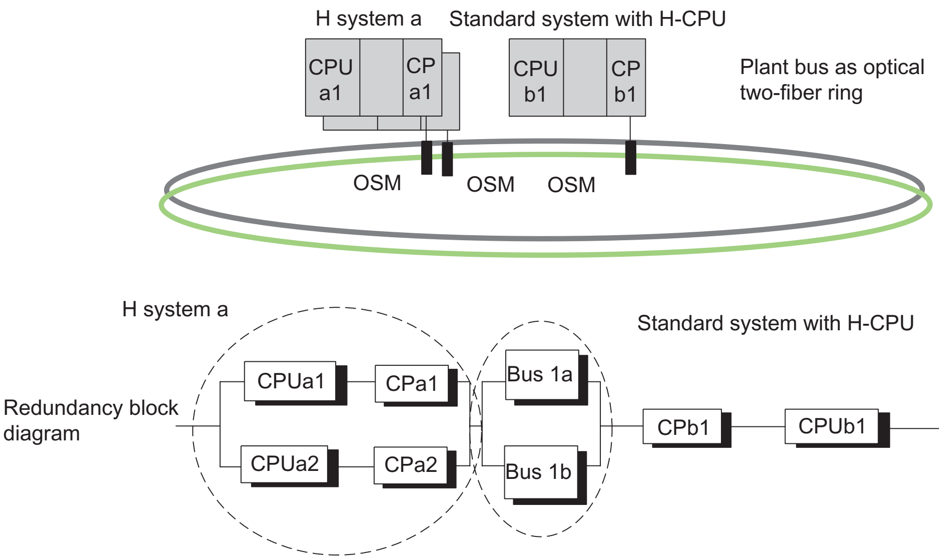


Figure 11-6 Example of redundancy with fault-tolerant system and fault-tolerant CPU

Reaction to failure

Double errors in the fault-tolerant system (in other words, CPUa1 and CPa2) or single errors in a standard system (CPUb1) lead to a total failure of communication between the systems involved; see previous figure.

11.5.3 Communication between fault-tolerant systems and PCs

Availability

When fault-tolerant systems are linked to a PC, the availability of the overall system is concentrated not only on the PCs (OS) and their data retention, but also on data acquisition on the automation systems.

PCs are not fault-tolerant, on account of their hardware and software characteristics. They can be configured redundantly within a system, however. The availability of this kind of PC (OS) system and its data management is ensured by means of suitable software such as WinCC Redundancy.

Communication take place via fault-tolerant connections.

The "S7-REDCONNECT" software package, V1.3 or higher, is essential for fault-tolerant communication on a PC. It supports the connection of a PC to a fiber-optic network with one CP, or to a redundant bus system with 2 CPs.

Configuring connections

The PC must be engineered and configured as a SIMATIC PC station. Additional project engineering of the fault-tolerant communication is not necessary at the PC end. Connection configuration is handled by the STEP 7 project in the form of an XDB file at the PC end.

You can find out how to use STEP 7 fault-tolerant S7 communication to integrate a PC into your OS system in the WinCC documentation.

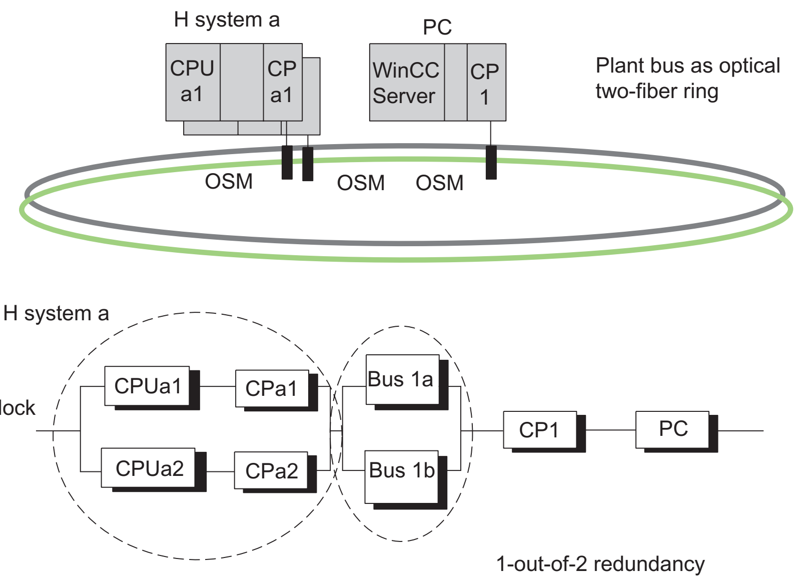


Figure 11-7 Example of redundancy with fault-tolerant system and redundant bus system

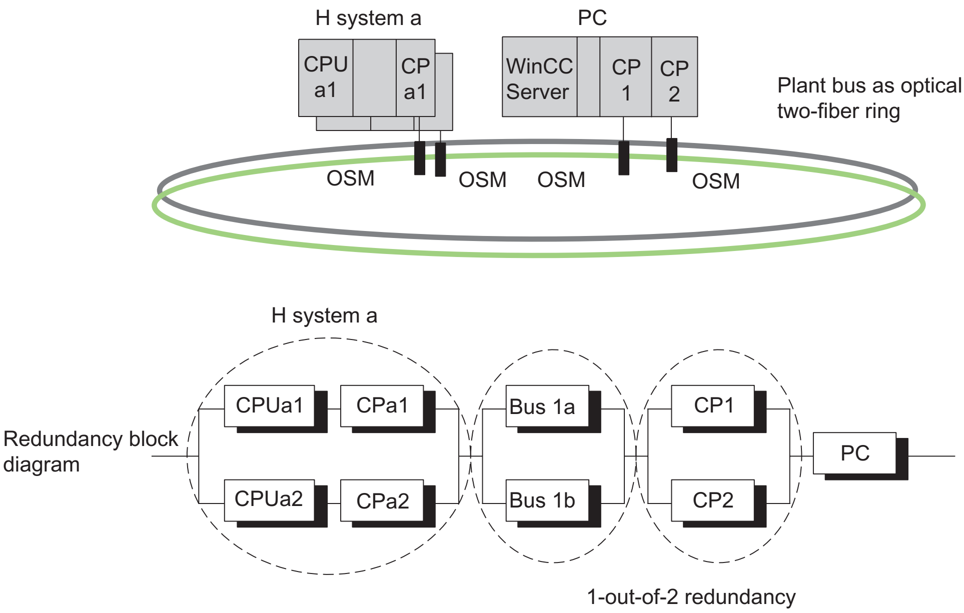


Figure 11-8 Example of redundancy with a fault-tolerant system, redundant bus system, and CP redundancy on PC.

Reaction to failure

Double errors in the fault-tolerant system (in other words, CPUa1 and CPa2) and the failure of the PC result in a total failure of communication between the systems involved (see previous figures).

PC / PG as engineering system (ES)

To be able to use a PC as an engineering system, you need to configure it under its name as a PC station in HW Config. The ES is assigned to a CPU and is capable of executing the STEP 7 functions on that CPU.

If the CPU fails, communication between the ES and the fault-tolerant system is also no longer possible.

11.6 Communication via S7 connections

Communication with standard systems

Fault-tolerant communication between fault-tolerant and standard systems is not supported. The following examples illustrate the actual availability of the communicating systems.

Configuration

S7 connections are configure in STEP 7.

Programming

All communication functions are supported for standard communication on a fault-tolerant system.

The communication SFBs are used in STEP 7 to program communication.

Note

The START and STOP communication functions act on exactly one CPU or on all CPUs of the fault-tolerant system (for more details refer to the *System Software for S7-300/400, System and Standard Functions* reference manual) reference manual.

NOTICE
Downloading connection configuration during operation
If you download a connection configuration during operation, any established connections could be aborted.

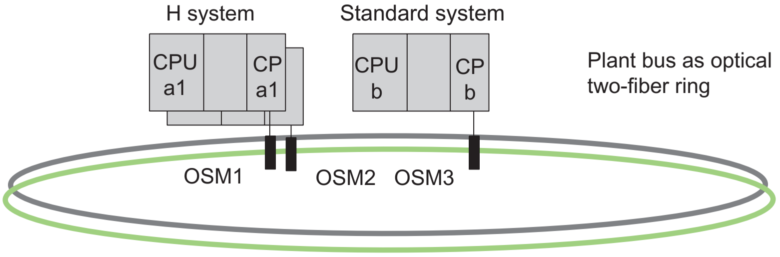
11.6.1 Communication via S7 connections - one-sided mode

Availability

Availability is likewise enhanced by using a redundant system bus for communications between fault-tolerant and standard systems.

On a system bus configured as multimode fiber optic ring, communication between the partner systems is maintained if the multimode fiber optic cable breaks. The systems then communicate as if they were connected to a bus system (linear structure); see following figure.

For linked fault-tolerant and standard systems, the availability of communication can not be improved by means of a dual electrical bus system. To be able to use the second bus system as a redundant system, you configure a second S7 connection and manage it accordingly in the user program (see figure after next).



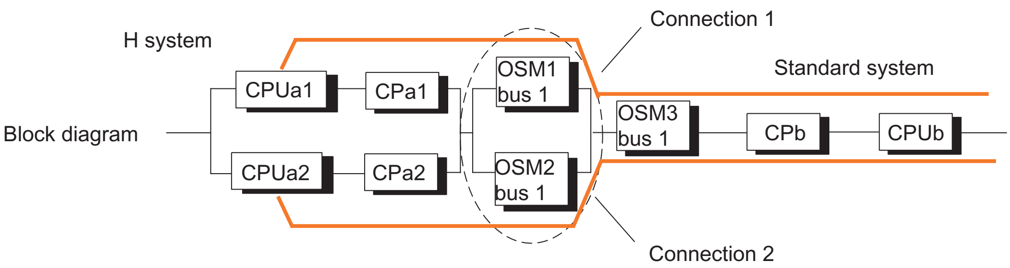


Figure 11-9 Example of linking of standard and fault-tolerant systems to a redundant ring

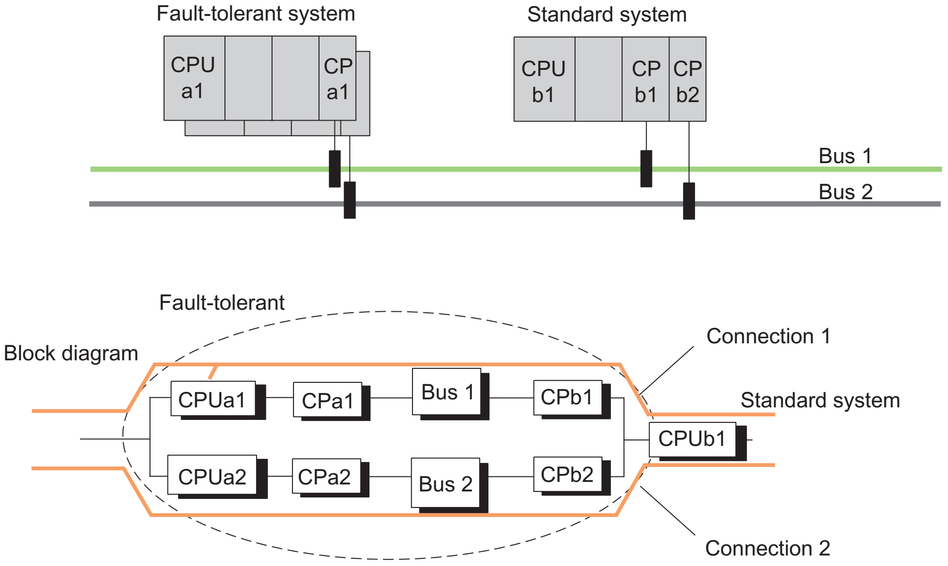


Figure 11-10 Example of linking standard and fault-tolerant systems to a redundant bus system

Reaction to failure

Two-fiber optical ring and bus system

Because standard S7 connections are used here (the connection ends at the CPU of the subsystem, in this case CPUa1), an error in the fault-tolerant system (e.g. CPUa1 or CPa1) or an error in system b (e.g. CP b) results in total failure of communication between the partner systems (see previous figures).

There are no bus system-specific differences in the reactions to failure.

Linking of standard and fault-tolerant systems

Driver block "S7H4_BSR": You can link an H system to an S7–400 using the "S7H4_BSR" driver block. For more detailed information, contact the H/F Competence Center

Telephone: +49 (911) 895-4759
Fax: +49 (911) 895-4519
E-mail: hf-cc.aud@siemens.com

Alternative: SFB 15 "PUT" and SFB 14 "GET" in the fault-tolerant system: As an alternative, use two SFB 15 "PUT" blocks over two standard connections. First call the first block. If there was no error message when the block executed, the transfer is assumed to have been successful. If there was an error message, the data transfer is repeated via the second block. If a connection abort is detected later, the data is also transferred again to exclude possible information losses. You can use the same method with an SFB 14 "GET".

If possible, use the mechanisms of S7 communication for communication.

11.6.2 Communication via redundant S7 connections

Availability

Availability can be enhanced by using a redundant system bus and two separate CPs on a standard system.

Redundant communication can also be operated with standard connections. For this two separate S7 connections must be configured in the program in order to implement connection redundancy. In the user program, both connections require the implementation of monitoring functions in order to allow the detection of failures and to change over to the standby connection.

The following figure shows such a configuration.

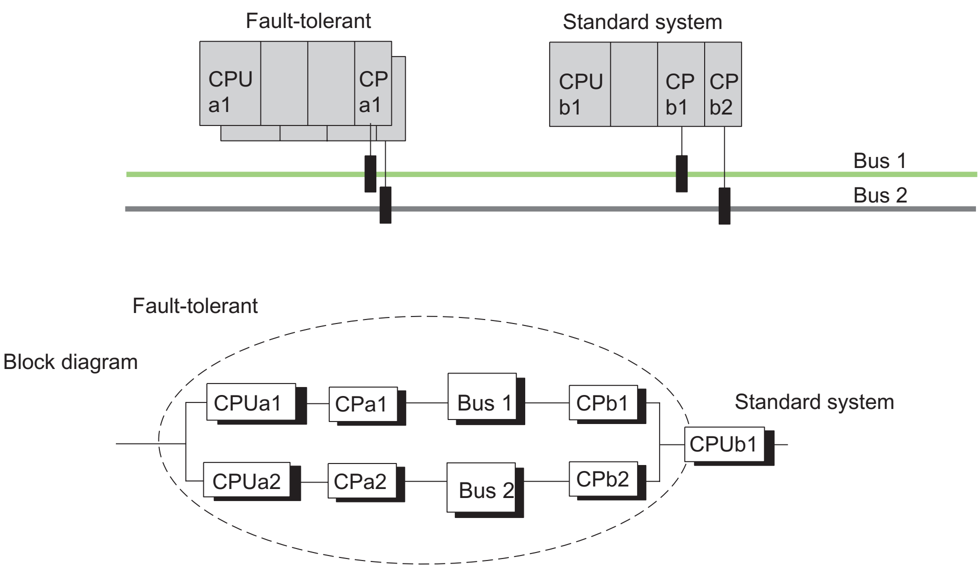


Figure 11-11 Example of redundancy with fault-tolerant systems and a redundant bus system with redundant standard connections

Reaction to failure

Double errors in the fault-tolerant system (in other words, CPUa1 and CPa 2) or in the standard system (CPb1 and CPb2), and single errors in the standard system (CPUb1) lead to a total failure of communication between the partners involved (see previous figure).

11.6.3 Communication via a point-to-point CP on the ET 200M

Connection via ET 200M

Links from fault-tolerant systems to single-channel systems are often possible only by way of point-to-point connections, as many systems have no other connection alternatives.

In order to make the data of a single-channel system available to CPUs of the fault-tolerant systems as well, the point-to-point CP (CP 341) must be installed in a distributed rack along with two IM 153-2 modules.

Configuring connections

Redundant connections between the point-to-point CP and the fault-tolerant system are not necessary.

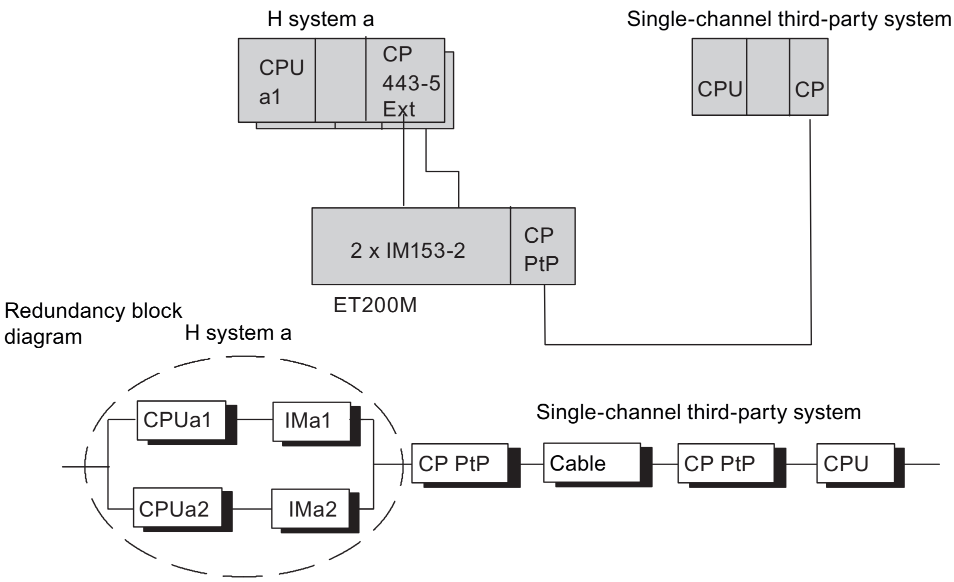


Figure 11-12 Example of linking of a fault-tolerant system and a single-channel third-party system

Reaction to failure

Double errors in the fault-tolerant system (in other words CPUa1 and IM153-2) and single errors in the third-party system lead to a total failure of communication between the systems involved (see previous figure).

The point-to-point CP can also be inserted centrally in "H system a". However, in this configuration even the failure of the CPU, for example, will cause a total failure of communication.

11.6.4 Custom linking to single-channel systems

Connection via PC as gateway

Fault-tolerant systems and single-channel systems can also be linked by a gateway (no connection redundancy). The gateway is linked to the system bus by one or two CPs, depending on availability requirements. Fault-tolerant connections can be configured between the gateway and the fault-tolerant systems. The gateway allows you to link any kinds of single-channel system (e.g. TCP/IP with a manufacturer-specific protocol).

A user-programmed software instance in the gateway implements the single-channel transition to the fault-tolerant systems, and so allows any single-channel system to be linked to a fault-tolerant system.

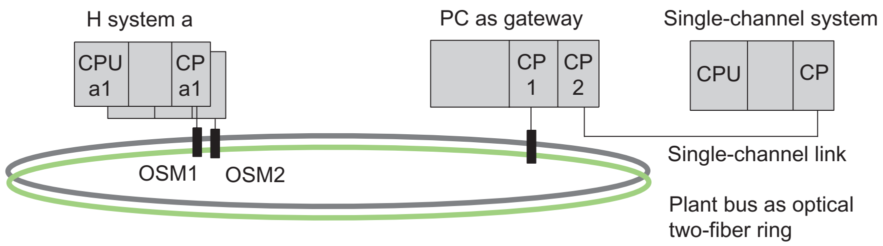
Configuring connections

Redundant connections between the gateway CP and the single-channel system are not required.

The gateway CP is located on a PC system which has fault-tolerant connections to the fault-tolerant system.

To configure fault-tolerant S7 connections between the fault-tolerant system A and the gateway, you first need to install S7-REDCONNECT on the gateway. The functions for preparing data for their transfer via the single-channel link must be implemented in the user program.

For further information, refer to the "*Industrial Communications IK10*" catalog.



Redundancy block diagram

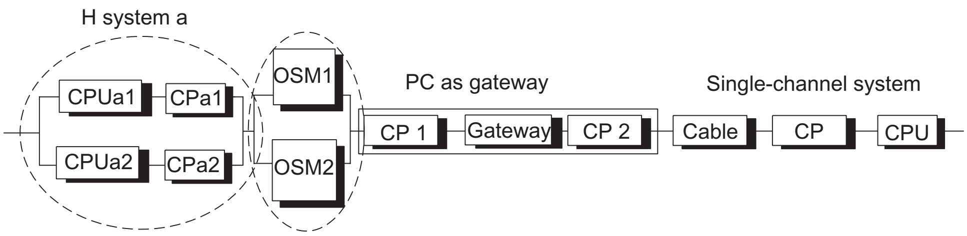


Figure 11-13 Example of linking of a fault-tolerant system to a single-channel external system

11.7 Communication performance

Compared to a fault-tolerant CPU in stand-alone mode or to a standard CPU, the communication performance (reaction time or data throughput) of a fault-tolerant system operating in redundant mode is significantly lower.

The aim of this description is to provide you with criteria which allow you to assess the effects of the various communication mechanisms on communication performance.

Definition of communication load

Communication load is the sum of requests per second issued to the CPU by the communication mechanisms, plus the requests and messages issued by the CPU.

Higher communication load increases the reaction time of the CPU, meaning the CPU takes more time to react to a request (such as a read request) or output requests and messages.

Operating range

In every automation system there is a linear operating range in which an increase in communication load will also lead to an increase in data throughput. This then results in reasonable reaction times which are acceptable for the automation task faced.

A further increase in communication load will push data throughput into the saturation range. Under certain conditions, the automation system may as a result be no longer be capable of processing the request volume within the response time demanded. Data throughput reaches its maximum, and the reaction time rises exponentially; see the figures below.

Data throughput may also be reduced by a certain amount due to additional internal loads inside the device.

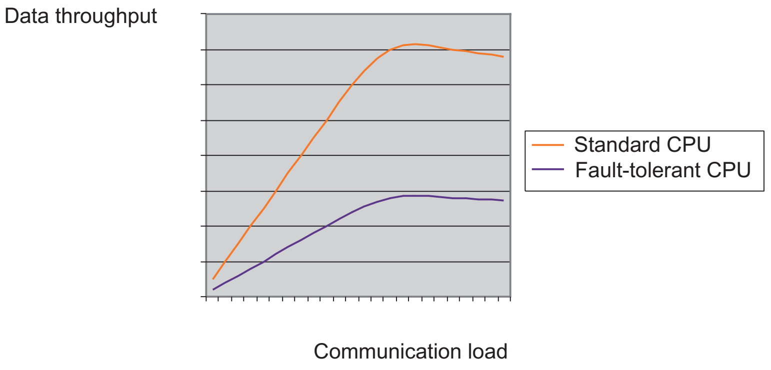


Figure 11-14 Communication load as a variable of data throughput (basic profile)

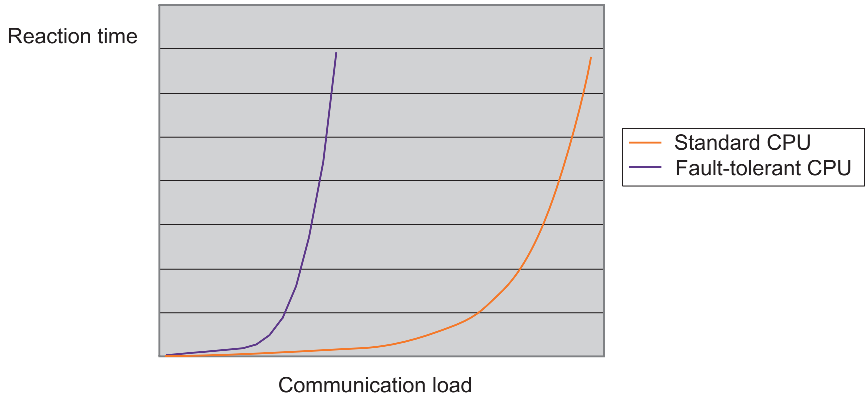


Figure 11-15 Communication load as a function of the response time (basic profile)

Standard and fault-tolerant systems

What we have said so far applies to standard and fault-tolerant systems. Since communication performance in standard systems is clearly higher than that of redundant H systems, saturation point will seldom be reached in today's plants.

In contrast, fault-tolerant systems always require synchronization to maintain parallel operation. This increases block execution times and reduces communication performance, This means that performance limits are reached earlier. If the redundant fault-tolerant system is not operating at its performance limits, the performance benchmark compared to the standard system will be lower by the factor 2 to 3.

Which variables influence communication load?

The communication load is affected by the following variables:

- Number of connections/connected OCM systems
- Number of tags, or number of tags in pictures displayed on OPs or using WinCC.
- Communication type (OCM, S7 communication, S7 message functions, S5-compatible communication, ...)
- The configured maximum cycle time extension as a result of communication load

The sections below show the factors that influence communication performance.

11.8 General issues in communication

Reduce the rate of communication request per second as far as possible. Utilize the maximum user data length for communication requests, for example by grouping several tags or data areas in one read request.

Each request requires a certain processing time, and its status should therefore not be checked before this process is completed.

You can download a tool for the assessment of processing times free of charge from the Internet at:

http://www4.ad.siemens.de/view/cs/de/1651770, article ID 1651770

Your calls of communication requests should allow the event-driven transfer of data. Check the data transfer event only until the request is completed.

Call the communication blocks sequentially and stepped down within the cycle, in order to obtain a balanced distribution of communication load.

You can by-pass the block call using a conditional jump if you do not transfer any user data.

A significant increase in communication performance between S7 components is achieved by using S7 communication functions, rather than S5-compatible communication functions.

As S5-compatible communication functions (FB "AG_SEND", FB "AG_RECV", AP_RED) generate a significantly higher communication load, you should only deploy these for the communication of S7 components with non-S7 components.

AP_Red software package

When using the "AP_RED" software package, limit the user data length to 240 bytes. If larger data volumes are necessary, transfer those in sequential block calls.

The "AP_RED" software package uses the mechanisms of FB "AG_SEND" and FB "AG_RCV". Use AP_RED only to link SIMATIC S5 / S5-H PLCs, or external devices which only support S5-compatible communication.

S7 communication (SFB 12 "BSEND" and SFB 13 "BRCV")

Do not call SFB 12 "BSEND" in the user program more often than the corresponding SFB 13 "BRCV" at the communication partner.

S7 communication (SFB 8 "USEND" and SFB 9 "URCV")

SFB 8 "USEND" should always be event-driven, because this block may generate a high communication load.

Do not call SFB 8 "USEND" in the user program more often than the corresponding SFB 9 "URCV" at the communication partner.

SIMATIC OPs, SIMATIC MPs

Do not install more than 4 OPs or 4 MPs in a fault-tolerant system. If you do need more OPs/MPs, your automation task may have to be revised. Contact your SIMATIC sales partner for support.

Do not select a screen refresh cycle time of less than 1s, and increase it to 2 s as required.

Verify that all screen tags are requested within the same cycle time, in order to form an optimized group for read requests.

OPC servers

When OPC was used to connect several HMI devices for your visualization tasks to a fault-tolerant system, you should keep the number of OPC servers accessing the fault-tolerant system as low as possible. OPC clients should always address a shared OPC server, which then fetches the data from the fault-tolerant system.

You can tune data exchange by using WinCC and its client/server concept.

Various HMI devices of third-party vendors support the S7communication protocol. You should utilize this option.

12 Configuring with STEP 7

12.1 Configuring with STEP 7

This section provides an overview of fundamental issues to be observed when you configure a fault-tolerant system.

The second section covers the PG functions in STEP 7.

For detailed information, refer to *Configuring fault-tolerant systems* in the basic help.

12.2 Configuring with STEP 7

The basic approach to configuring the S7-400H is no different from that used to configure the S7-400 - in other words:

- creating projects and stations
- configuring hardware and networking
- loading system data onto the PLC

Even the different steps that are required for this are identical for the most part to those familiar from the S7-400.

NOTICE
OBs required Always download these error OBs to the S7-400H CPU: OB 70, OB 72, OB 80, OB 82, OB 83, OB 85, OB 86, OB 87, OB 88, OB 121 and OB 122. If you ignore this, the fault-tolerant CPU goes into STOP when an error occurs.

Creating a fault-tolerant station

The SIMATIC fault-tolerant station ('H' station) represents a separate station type in SIMATIC Manager. It allows the configuration of two central units, each having a CPU and therefore a redundant station configuration.

12.2.1 Rules for the assembly of fault-tolerant stations

The following rules have to be complied with for a fault-tolerant station, in addition to the rules that generally apply to the arrangement of modules in the S7-400:

- The CPUs always have to be inserted in the same slots.
- Redundantly used external DP master interfaces or communication modules must be inserted in the same slots in each case.
- External DP master interface modules for redundant DP master systems should only be inserted in central units, rather than in expansion units.
- Redundantly used modules (for example, CPU 417-4H, DP slave interface module IM 153-2) must be identical, i.e. they must have the same order number, the same version, and the same firmware version.

Installation rules

- A fault-tolerant station may contain up to 20 expansion racks.
- Even-numbered mounting racks can be assigned only to central unit 0, whereas odd-numbered mounting racks can be assigned only to central unit 1.
- Modules with communication bus interface can be operated only in mounting racks 0 through 6.
- Communication-bus capable modules are not permissible in switched I/Os.
- Pay attention to the mounting rack numbers when operating CPs for redundant communication in expansion racks:

  The numbers must be directly sequential and begin with the even number - for example, mounting racks numbers 2 and 3, but not mounting racks numbers 3 and 4.
- A rack number is also assigned for DP master no. 9 onwards if the central unit contains DP master modules. The number of possible expansion racks is reduced as a result.

Compliance with the rules is monitored automatically by STEP 7 and taken into account in an appropriate manner during configuration.

12.2.2 Configuring hardware

The simplest way of achieving a redundant hardware configuration consists in initially equipping **one** rack with all the redundant components, assigning parameters to them and then copying them.

You can then specify the various addresses (for one-sided I/Os only!) and arrange other, non-redundant modules in individual racks.

Special features in presenting the hardware configuration

In order to enable quick recognition of a redundant DP master system, it is represented by two closely parallel DP cables.

12.2.3 Assigning parameters to modules in a fault-tolerant station

Introduction

Assigning parameters to modules in a fault-tolerant station is no different from assigning parameters to modules in S7-400 standard stations.

Procedure

All the parameters of the redundant components (with the exception of MPI and communication addresses) must be identical.

The special case of CPUs

You can only edit the CPU0 parameters (CPU on rack 0). Any values that you specify for it are automatically allocated to CPU1 (CPU on rack 1). The settings of CPU1 can not be changed, with the exception of the following parameters:

- MPI address of the CPU
- CPU name, plant designation, location ID

Configuring modules addressed in the I/O address space

Always configure a module that is addressed in the I/O address space so that it is located either entirely in the process image or entirely outside.

Otherwise, consistency can not be guaranteed, and the data may be corrupted.

I/O access using word or dword statements

The system loads the values to accumulator "0" if the word or dword for I/O access contains only the first or the first three bytes, but not the remaining bytes of the address space.

Example: The I/O is at address 8 and 9 in the S7-400H CPU; addresses 10 and 11 are not used. Access L ID 8 causes the system to load the value DW#16#00000000 into the accumulator.

12.2.4 Recommendations for setting the CPU parameters

CPU parameters that determine cyclic behavior

You specify the CPU parameters that determine the cyclic behavior of the system on the "Cycle/Clock memory" tab.

Recommended settings:

- As long a scan cycle monitoring time as possible (e.g.6000 ms)
- OB 85 call when there is an I/O access error: only with incoming and outgoing errors

Number of messages in the diagnostics buffer

You specify the number of messages in the diagnostics buffer on the "Diagnostics/Clock" tab.

We recommend that you set a large number (1500, for example).

Monitoring time for transferring parameters to modules

You specify this monitoring time on the "Startup" tab. It depends on the configuration of the fault-tolerant station. If the monitoring time is too short, the CPU enters the W#16#6547 event in the diagnostics buffer.

For some slaves (e.g. IM 157) these parameters are packed in system data blocks. The transmission time of the parameters depends on the following factors:

- Baud rate of the bus system (high baud rate => short transmission time)
- Size of the parameters and the system data blocks (long parameter => long transmission time)
- Load on the bus system (many slaves => long transmission time);
  Note: The bus load is at its peak during restart of the DP master, for example following Power OFF/ON

Recommended setting: 600 corresponds to 60 s.

Note

The specifically fault-tolerant CPU parameters, and so also the associated monitoring times, are calculated automatically. This involves setting a default value for the total memory load of all data blocks specifically for a CPU. If your fault-tolerant system does not link up, check the work memory assignment (HW Config > CPU Properties > H Parameters > Work memory used for all data blocks).

NOTICE
A CP 443-5 Extended (order number 6GK7443–5DX03) may only be used for transmission rates of 1.5 Mbps in an S7-400H or S7–400FH when a DP/PA– or Y–Link is connected (IM157, order number 6ES7157-0AA00-0XA0, 6ES7157-0AA80-0XA0, 6ES7157-0AA81-0XA0). Remedy: see FAQ 11168943 at http://www.siemens.com/automation/service&support.

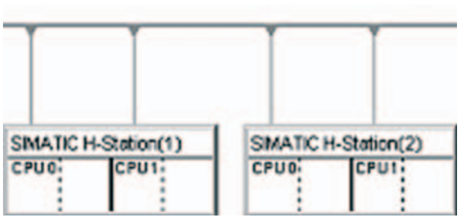
12.2.5 Configuring networking

The fault-tolerant S7 connection is a separate connection type of the "Configure Networks" application. The following communication partners can communicate with each other:

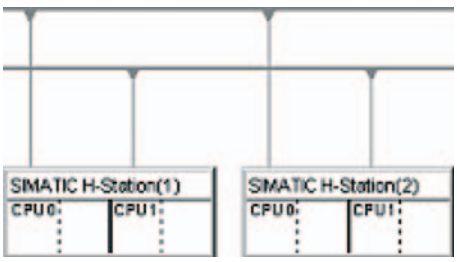
- S7–400 H station (with 2 fault-tolerant CPUs) -> S7–400 H station (with 2 fault-tolerant CPUs)
- S7–400 H station (with 1 fault-tolerant CPU) -> S7–400 H station (with 2 fault-tolerant CPUs)
- S7–400 H station (with 1 fault-tolerant CPU) -> S7–400 H station (with 1 fault-tolerant CPU)
- SIMATIC PC stations -> S7–400 H station (with 2 fault-tolerant CPUs)

When this type of connection is being configured, the application automatically determines the number of possible connection paths:

- If two independent but identical subnets are available which are both suitable for an S7 connection (DP master systems), two connection paths will be used. In practice these are generally electrical networks, each a CP in a subnet:



- If only one DP master system is available - in practice typically fiber-optic cables - four connection paths are used for a connection between two fault-tolerant stations. All the CPs are in this subnet:



Downloading the network configuration to the fault-tolerant station

The network configuration can be downloaded to the entire fault-tolerant station in one pass. To do this, the same requirements must be met as for downloading the network configuration to a standard station.

12.3 Programming device functions in STEP 7

Display in SIMATIC Manager

In order to do justice to the special features of a fault-tolerant station, the way in which the system is visualized and edited in SIMATIC Manager differs from that of a S7-400 standard station as follows:

- In the offline view, the S7 program appears only under CPU0 of the fault-tolerant station. No S7 program is visible under CPU1.
- In the online view, the S7 program appears under both CPUs and can be selected in both locations.

Communication functions

For programming device (PG) communication functions such as downloading and deleting blocks, one of the two CPUs has to be selected even if the function affects the entire system over the redundant link.

- Data which are modified in one of the central processing units in redundant operation affect the other CPUs over the redundant link.
- Data which are modified when there is no redundant link - in other words, in single mode - initially affect only the edited CPU. The blocks are applied by the master CPU to the standby CPU during the next link-up and update. Exception: After a configuration modification no new blocks are applied (only the unchanged data blocks). Loading the blocks is then the responsibility of the user.

Failure and replacement of components during operation 13

13.1 Failure and replacement of components during operation

One factor that is crucial to the uninterrupted operation of the fault-tolerant PLC is the replacement of failed components in ongoing operation (run mode). Quick repairs will recover fault-tolerant redundancy.

We will show you in the sections that follow how simple and fast it can be to repair and replace components in the S7-400H. Also refer to the tips in the corresponding sections of the installation manual, *S7-400 Programmable Controllers, Hardware and Installation*

13.2 Failure and replacement of components during operation

Which components can be replaced?

The following components can be replaced during operation:

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

13.2.1 Failure and replacement of a CPU

Complete replacement of the CPU is not always necessary. If only load memory fails, it is enough to replace the corresponding memory module. Both cases are described below.

Starting situation for replacement of the CPU

Failure	How does the system react?
The S7-400H is in redundant mode and a **CPU** fails.	• Partner CPU switches to single mode. • The partner CPU reports the event in the diagnostics buffer and in OB 72.

Requirements for replacement

The module replacement described below is possible only if the "new" CPU

- has the same operating system version as the failed CPU and
- if it is equipped with the same load memory as the failed CPU.

NOTICE

New CPUs are always shipped with the latest operating system version. If this differs from the version of the operating system of the remaining CPU, you will have to equip the new CPU with the same version of the operating system. Either create an operating system update card for the new CPU and use this to load the operating system on the CPU or load the required operating system in HW Config with "PLC -> Update Firmware", see section Updating the firmware without a memory card (Page 61).

Procedure

Follow the steps below to **replace a CPU**:

Step	What needs to be done?	How does the system react?
1	Turn off the power supply module.	• The entire subsystem is switched off (system operating in single mode).
2	Replace the CPU. Make sure the rack number is set correctly on the CPU.	–
3	Insert the synchronization modules.	–
4	Plug in the fiber-optic cable connections of the synchronization modules.	–
5	Switch the power supply module on again.	• CPU runs the self-tests and changes to STOP.
6	Perform a CPU memory reset on the replaced CPU.	–
7	Start the replaced CPU (for example STOP³RUN or Start using the PG).	• CPU performs automatic LINK-UP and UPDATE. • CPU changes to RUN and operates as the standby CPU.

Starting situation for replacement of the load memory

Failure	How does the system react?
The S7-400H is in redundant mode and a **load memory access error** occurs.	• The relevant CPU changes to STOP and requests a memory reset. • Partner CPU switches to single mode.

Procedure

Follow the steps below to **replace the load memory**:

Step	What needs to be done?	How does the system react?
1	Replace the memory card on the stopped CPU.	–
2	Perform a memory reset on the CPU with the replaced memory card.	–
3	Start the CPU.	• CPU performs automatic LINK-UP and UPDATE. • CPU changes to RUN and operates as the standby CPU.

13.2.2 Failure and replacement of a power supply module

Starting situation

Both CPUs are in RUN.

Failure	How does the system react?
The S7-400H is in redundant mode and a power supply module fails.	• Partner CPU switches to single mode. • The partner CPU reports the event in the diagnostics buffer and in OB 72.

Procedure

To replace a power supply module in the central rack:

Step	What needs to be done?	How does the system react?
1	Turn off the power supply (24 V DC for PS 405 or 120/230 V AC for PS 407).	• The entire subsystem is switched off (system operating in single mode).
2	Replace the module.	–
3	Switch the power supply module on again.	• CPU executes the self-tests. • CPU performs automatic LINK-UP and UPDATE. • CPU changes to RUN (redundant mode) and operates as the standby CPU.

Note

Redundant power supply

If you use a redundant power supply (PS 407 10A R), two power supply modules are assigned to one fault-tolerant CPU. If a part of the redundant PS 407 10A R power supply module fails, the corresponding CPU keeps on running. The defective part can be replaced during operation.

Other power supply modules

If the failure concerns a power supply module outside the central rack (e.g. in the expansion rack or in the I/O device) the failure is reported as a rack failure (central) or station failure (remote). In this case, simply switch off the power supply to the power supply module concerned.

13.2.3 Failure and replacement of an input/output or function module

Starting situation

Failure	How does the system react?
The S7-400H is in redundant mode and a input/output or function module fails.	• Both CPUs report the event in the diagnostics buffer and via appropriate OBs.

Procedure

CAUTION

Note the different procedures.

Minor injury or damage to equipment is possible.

The procedure for replacing and input/output or function module differs for modules of the S7-300 and S7-400.

Use the correct procedure when replacing a module. The correct procedure is described below for the S7-300 and the S7-400.

To replace signal and function modules of an S7-300, perform the following steps:

Step	What needs to be done?	How does the system react?
1	Remove the failed module (in RUN mode).	• Both CPUs process the insert/remove-module interrupt OB 83 synchronized with each other.
2	Disconnect the front connector and wiring.	• Call OB 82 if the module concerned is is capable of diagnostic interrupts and diagnostic interrupts are enabled in the configuration. • Call OB 122 if you are accessing the module by direct access • Call OB 85 if you are accessing the module using the process image
3	Plug the front connector into the new module.	• Call OB 82 if the module concerned is is capable of diagnostic interrupts and diagnostic interrupts are enabled in the configuration.
4	Insert the new module.	• Both CPUs process the insert/remove-module interrupt OB 83 synchronized with each other. • Parameters are assigned automatically to the module by the CPU concerned and the module is addressed again.

To replace signal and function modules of an S7-400, perform the following steps:

Step	What needs to be done?	How does the system react?
1	Disconnect the front connector and wiring.	• Call OB 82 if the module concerned is is capable of diagnostic interrupts and diagnostic interrupts are enabled in the configuration. • Call OB 122 if you are accessing the module by direct access • Call OB 85 if you are accessing the module using the process image
2	Remove the failed module (in RUN mode).	• Both CPUs process the insert/remove-module interrupt OB 83 synchronized with each other.
3	Insert the new module.	• Both CPUs process the insert/remove-module interrupt OB 83 synchronized with each other. • Parameters are assigned automatically to the module by the CPU concerned and the module is addressed again.
4	Plug the front connector into the new module.	• Call OB 82 if the module concerned is is capable of diagnostic interrupts and diagnostic interrupts are enabled in the configuration.

13.2.4 Failure and replacement of a communication module

This section describes the failure and replacement of communication modules for PROFIBUS and Industrial Ethernet.

The failure and replacement of communications modules for PROFIBUS DP are described in section Failure and replacement of a PROFIBUS-DP master (Page 214).

Starting situation

Failure	How does the system react?
The S7-400H is in redundant mode and a communication module fails.	• Both CPUs report the event in the diagnostics buffer and via appropriate OBs. • In communication via standard connections: Connection failed • In communication via redundant connections: Communication is maintained without interruption over an alternate channel.

Procedure

To replace a communication module for PROFIBUS or Industrial Ethernet:

Step	What needs to be done?	How does the system react?
1	Extract the module.	• Both CPUs process the insert/remove-module interrupt OB 83 synchronized with each other.
2	Make sure that the new module has no parameter data in its integrated FLASH EPROM and plug it in.	• Both CPUs process the insert/remove-module interrupt OB 83 synchronized with each other. • The module is automatically configured by the appropriate CPU.
3	Turn the module back on.	• The module resumes communication (system establishes communication connection automatically).

13.2.5 Failure and replacement of a synchronization module or fiber-optic cable

In this section, you will see three different error scenarios:

- Failure of a synchronization module or fiber-optic cable
- Successive failure of the two synchronization modules or fiber-optic cables
- Simultaneous failure of the two synchronization modules or fiber-optic cables

The CPU displays by means of LEDs and by means of the diagnosis whether the lower or upper redundant link has failed. After the defective parts (fiber-optic cable or synchronization module) have been replaced, LEDs IFM1F and IFM2F go out.

Starting situation

Failure	How does the system react?
Failure of a fiber-optic cable or synchronization module: The S7-400H is in redundant mode and a fiber-optic cable or a synchronization module fails.	• Master CPU reports the event in the diagnostic buffer and with OB 72. • Master CPU remains in RUN mode; standby CPU changes to STOP • The diagnostic LED on the synchronization module is lit

Procedure

Follow the steps below to replace a synchronization module or fiber-optic cable:

Step	What needs to be done?	How does the system react?
1	First, check the fiber-optic cable.	–
2	Start the standby CPU (for example, STOP-RUN or Start using the PG).	The following reactions are possible: 1. CPU changes to RUN mode. 2. CPU changes to STOP mode. In this case continue at step 3.
3	Remove the faulty synchronization module from the standby CPU.	–
4	Insert the new synchronization module in the standby CPU.	–
5	Plug in the fiber-optic cable connections of the synchronization modules.	• The diagnostic LED on the synchronization module goes off • Both CPUs report the event in the diagnostic buffer
6	Start the standby CPU (for example, STOP-RUN or Start using the PG).	The following reactions are possible: 1. CPU changes to RUN mode. 2. CPU changes to STOP mode. In this case continue at step 7.
7	If the standby CPU changed to STOP in step 6: Remove the synchronization module from the master CPU.	• Master CPU processes insert/remove-module interrupt OB 83 and redundancy error OB 72 (entering state).

Step	What needs to be done?	How does the system react?
8	Insert the new synchronization module into the master CPU.	• Master CPU processes insert/remove-module interrupt OB 83 and redundancy error OB 72 (exiting state).
9	Plug in the fiber-optic cable connections of the synchronization modules.	–
10	Start the standby CPU (for example, STOP-RUN or Start using the PG).	• CPU performs automatic LINK-UP and UPDATE. • CPU changes to RUN (redundant mode) and operates as the standby CPU.

Note

If both fiber-optic cables or synchronization modules are damaged or replaced one after the other, the system reactions are the same as described above.

The only exception is that the standby CPU does not change to STOP but instead requests a memory reset.

Starting situation

Failure	How does the system react?
Failure of both fiber-optic cables or synchronization modules: The S7-400H is in redundant mode and **both** fiber-optic cables or synchronization modules fail.	• Both CPUs report the event in the diagnostic buffer and with OB 72. • Both CPUs become the master CPU and remain in RUN mode. • The diagnostic LED on the synchronization module is lit

Procedure

The double error described results in loss of redundancy. In this event proceed as follows:

Step	What needs to be done?	How does the system react?
1	Switch off one subsystem.	–
2	Replace the faulty components.	–
3	Turn the subsystem back on.	• LEDs IFM1F and IFMF2F go off. The standby LED lights up.
4	Start the CPU (for example Start from programming device or STOP³RUN).	• CPU performs automatic LINK-UP and UPDATE. • CPU changes to RUN (redundant mode) and operates as the standby CPU.

Failure and replacement of an IM 460 and IM 461 interface module

The IM 460 and IM 461 interface modules provide functions for connecting expansion modules.

Starting situation

Failure	How does the system react?
The S7-400H is in redundant mode and an interface module fails.	• The connected expansion unit is turned off. • Both CPUs report the event in the diagnostic buffer and with OB 86.

Procedure

Follow the steps below, to replace an interface module:

Step	What needs to be done?	How does the system react?
1	Turn off the power supply of the central unit.	• The partner CPU switches to single mode.
2	Turn off the power supply of the expansion unit in which you want to replace the interface module.	–
3	Remove the interface module.	–
4	Insert the new interface module and turn the power supply of the expansion unit back on.	–
5	Switch the power supply of the central unit back on and start the CPU.	• CPU performs automatic LINK-UP and UPDATE. • CPU changes to RUN and operates as the standby CPU.

13.2.6 Failure and replacement of an IM 460 and IM 461 interface module

Starting situation

Failure	How does the system react?
The S7-400H is in redundant mode and an interface module fails.	• The connected expansion unit is turned off. • Both CPUs report the event in the diagnostic buffer and with OB 86.

Procedure

Follow the steps below, to replace an interface module:

Step	What needs to be done?	How does the system react?
1	Turn off the power supply of the central unit.	• The partner CPU switches to single mode.
2	Turn off the power supply of the expansion unit in which you want to replace the interface module.	–
3	Remove the interface module.	–
4	Insert the new interface module and turn the power supply of the expansion unit back on.	–
5	Switch the power supply of the central unit back on and start the CPU.	• CPU performs automatic LINK-UP and UPDATE. • CPU changes to RUN and operates as the standby CPU.

13.3 Failure and replacement of components of the distributed I/Os

Which components can be replaced?

The following components of the distributed I/Os can be replaced during operation:

- PROFIBUS-DP master
- PROFIBUS-DP interface module (IM 153-2 or IM 157)
- PROFIBUS-DP slave
- PROFIBUS-DP cable

Note

Replacing I/O and function modules located in a distributed station is described in Section Failure and replacement of an input/output or function module (Page 205).

13.3.1 Failure and replacement of a PROFIBUS-DP master

Starting situation

Failure	How does the system react?
The S7-400H is in redundant mode and a DP master module fails.	• With single-channel, one-sided I/O: DP master can no longer process connected DP slaves. • With switched I/O: DP slaves are addressed via the DP master of the partner.

Procedure

To replace a PROFIBUS-DP master:

Step	What has to be done?	How does the system react?
1	Turn off the power supply of the central rack.	The fault-tolerant system switches to single mode.
2	Unplug the Profibus–DP cable of the affected DP master module.	–
3	Replace the affected module.	–
4	Plug the Profibus–DP cable back in.	–
5	Turn on the power supply of the central rack.	• CPU performs automatic LINK-UP and UPDATE. • CPU changes to RUN and operates as the standby CPU.

13.3.2 Failure and replacement of a redundant PROFIBUS-DP interface module

Starting situation

Failure	How does the system react?
The S7-400H is in redundant mode and a PROFIBUS-DP interface module (IM 153–2, IM 157) fails.	Both CPUs report the event in the diagnostics buffer and via OB 70.

Replacement procedure

To replace the PROFIBUS-DP interface module:

Step	What has to be done?	How does the system react?
1	Turn off the supply for the affected DP interface module.	–
2	Unplug the connected bus connector.	–
3	Insert the new PROFIBUS-DP interface module and turn the supply back on.	–
4	Plug the bus connector back in.	• CPUs process the rack failure OB 70 in synchronism (outgoing event). • Redundant access to the station is again possible for the system.

13.3.3 Failure and replacement of a PROFIBUS-DP slave

Starting situation

Failure	How does the system react?
The S7-400H is in redundant mode and a DP slave fails.	Both CPUs report the event in the diagnostics buffer and via the appropriate OB.

Procedure

To replace a DP slave:

Step	What has to be done?	How does the system react?
1	Turn off the supply for the DP slave.	–
2	Unplug the connected bus connector.	–
3	Replace the DP slave.	–
4	Plug the bus connector in and turn the supply back on.	• CPUs process the rack failure OB 86 in synchronism (outgoing event) • DP slave can be addressed by the relevant DP master system.

13.3.4 Failure and replacement of PROFIBUS-DP cables

Starting situation

Failure	How does the system react?
The S7-400H is in redundant mode and the PROFIBUS-DP cable is defective.	• With single-channel, one-sided I/O: Rack failure OB (OB 86) is started (incoming event). DP master can no longer process connected DP slaves (station failure). • With switched I/O: I/O redundancy error OB (OB 70) is started (incoming event). DP slaves are addressed via the DP master of the partner.

Replacement procedure

To replace the PROFIBUS-DP cables:

Step	What has to be done?	How does the system react?
1	Check the wiring and localize the interrupted PROFIBUS-DP cable.	–
2	Replace the defective cable.	–
3	Switch the failed modules to RUN.	CPUs process error OBs in synchronism • With one-sided I/O: Rack failure OB 86 (outgoing event) DP slaves can be addressed via the DP master system. • With switched I/O: I/O redundancy error OB70 (outgoing event). DP slaves can be addressed via both DP master systems.

14 System modifications in operation

14.1 System modifications in operation

In addition to the options of hot-swapping of failed components as described in section Failure and replacement of components during operation (Page 201), you can also make changes to the plant in an H system without interrupting the running of the program.

The procedure depends on whether you are working on your user software in PCS 7 or STEP 7.

The procedures described below for changes during operation are designed so that you start with the redundant mode (see section The system states of the S7-400H (Page 87)) with the aim of returning to this mode when the procedures are completed.

NOTICE
Keep strictly to the rules described in this section with regard to modifications of the system in runtime. If you contravene one or more rules, the response of the fault-tolerant system can result in its availability being restricted or even failure of the entire programmable logic controller. Only perform a system change in runtime when there is no redundancy error, in other words, when the REDF LED is not lit. The automation system may otherwise fail. The cause of a redundancy error is listed in the diagnostics buffer.

Security-relevant components are not taken into account in this description. For more details of dealing with fail-safe systems refer to the *S7-400F and S7-400FH Programmable Controllers* manual.

14.2 Possible hardware modifications

How is a hardware modification made?

If the hardware components concerned are suitable for unplugging or plugging in live, the hardware modification can be carried out in the redundant state. However, the fault-tolerant system must be operated temporarily in single mode, because any download of new hardware configuration data in redundant mode would inevitably cause it to STOP. The process is then controlled only by one CPU, while you can carry out the relevant changes at the partner CPU.

WARNING
During a hardware modification, you can either remove or add modules. If you want to alter your fault-tolerant system in such a that you remove some modules and add others, you have to make two hardware changes.

NOTICE
Always download configuration changes to the CPU using the "Configure hardware" function.

Load memory data of the redundant CPUs must be updated several times in the process. It is therefore advisable to expand the integrated load memory with a RAM module, at least temporarily.

You may only change the FLASH card to a RAM card as required for this if the FLASH card has as much maximum storage space as the largest RAM card available. If you can not obtain a RAM module with a capacity to match the FLASH memory space, split the relevant actions in your configuration and program modifications into several smaller steps, in order to provide sufficient space in the integrated load memory.

Synchronization link

Whenever you make hardware modifications, make sure that the synchronization link between the two CPUs is established **before** you start or turn on the standby CPU. If the power supply to the CPUs is on, the LEDs IFM1F and IFM2F that indicate errors on the module interfaces on the two CPUs should **go off**.

If one of the IFM LEDs lights up again, even after you have replaced the relevant synchronization modules, the synchronization cables and even the standby CPU, there is a problem on the master CPU. In this case, you can, however, switch to the standby CPU by selecting the "via only one intact redundancy link" option in the "Switch" STEP 7 dialog box.

Which components can be modified?

The following modifications can be made to the hardware configuration during operation:

- Adding or removing modules to/from the central or expansion units (e.g. one-sided I/O module).

NOTICE
Always switch off the power before you install or remove the IM460 and IM461 interface modules, external CP443-5 Extended DP master interface module and their connecting cables.

- Adding or removing components of the distributed I/Os, such as
  - DP slaves with a redundant interface module (e.g. ET 200M, DP/PA link or Y link)
  - One-sided DP slaves (in any DP master system)
  - Modules in modular DP slaves
  - DP/PA links
  - PA devices
- Changing specific CPU parameters
- Changing the CPU memory configuration
- Reconfiguration of a module
- Assigning a module to another process image partition
- Upgrading the CPU version
- Changing master with only one more available redundant link.

When you make any modifications, keep to the rules for the configuration of a fault-tolerant station (see section Rules for the assembly of fault-tolerant stations (Page 27)).

What should I note at the system planning stage?

For switched I/Os to be expanded during operation the following points must be taken into account at the system planning stage:

- In both cables of a redundant DP master system sufficient numbers of branching points are to be provided for spur lines or isolating points (spur lines are not permitted at transmission rates of 12 Mbps). This may either be done at regular intervals or at all well accessible points.
- Both cables must be uniquely identified so that the line which is currently active is not accidentally cut off. This identification should be visible not only at the end points of a line but also at each possible new connection point. Different colored cables are excellent for this.
- Modular DP slave stations (ET 200M), DP/PA links and Y links must always be installed with an active backplane bus and fitted with all the bus modules required wherever possible, because the bus modules can not be installed and removed during operation.
- Always terminate both ends of PROFIBUS DP and PROFIBUS PA bus cables using active bus terminators in order to ensure proper termination of the cables while you are reconfiguring the system.
- PROFIBUS PA bus systems should be built up using components from the SpliTConnect product range (see interactive catalog CA01) so that separation of the lines is not required.
- Loaded data blocks must not be deleted and created again. In other words, SFC 22 (CREATE_DB) and SFC 23 (DEL_DB) may not be applied to DB numbers occupied by loaded DBs.
- Always ensure that the current status of the user program is available as a STEP 7 project in block format at the PG/ES when you modify the system configuration. It is not enough to upload the user program from one of the CPUs to the PG/ES, or to compile the code again from an STL source.

Modification of the hardware configuration

With a few exceptions, all elements of the configuration can be modified during operation. Usually, any configuration changes will also affect the user program.

The following must not be modified:

- Certain CPU parameters (for details refer to the relevant subsections)
- The transmission rate (baud rate) of redundant DP master systems
- S7 and S7H connections

Modifications to the user program and the connection configuration

The modifications to the user program and the connection configuration are loaded into the PLC in the redundant mode. The procedure depends on the software used. For more details refer to the *Programming with STEP 7* manual and the *PCS 7, Configuration Manual*.

Note

After reloading connections / gateways, it is no longer possible to change from RAM card to to FLASH card.

Special features

- Keep changes to a manageable extent. We recommend that you modify only one DP master and/or a few DP slaves (e.g. no more than 5) per reconfiguration run.
- When using an IM 153-2, active bus modules can only be plugged in if the power supply is off.

NOTICE
Remember the following when using redundant I/O that you have implemented as one-sided I/O at the user level (see section Other options for connecting redundant I/Os (Page 164)): Due to the link-up and update process carried out after a system modification, the I/O data of the previous master CPU may be temporarily deleted from the process image until all (changed) I/Os of the "new" master CPU are written to the process image. During the first update of the process image after a system modification, you may (incorrectly) have the impression that the redundant I/O has failed completely or that a redundant I/O exists. So correct evaluation of the redundancy status is not possible until the process image has been fully updated. This phenomenon does not occur with modules that have been enabled for redundant operation (see section Connecting redundant I/Os (Page 138)).

Preparations

To minimize the time during which the fault-tolerant system has to run in single mode, you should perform the following steps **before** making the hardware change:

- Check whether the CPUs provide sufficient memory capacity for the new configuration data and user program. If necessary, first expand the memory configuration (see section Changing the CPU memory configuration (Page 266)).
- Always ensure that plugged modules which are not configured yet do not have any unwanted influence on the process.

Procedure

Follow the steps below for any system change during operation:

1. Make the changes in HW Config.
2. Download the changed engineering to the CPU in STOP
3. Make the system change as described in the following sections.
4. Do not save the modified project engineering until the modification has been completed successfully.

14.3 Adding components in PCS 7

Starting situation

You have verified that the CPU parameters, such as monitoring times, match the planned new program. If they do not, adapt the CPU parameters first (see section Editing CPU parameters (Page 260)).

The fault-tolerant system is operating in redundant mode.

Procedure

Carry out the steps listed below to add hardware components to a fault-tolerant system in PCS 7. Details of each step are listed in a subsection.

Step	What needs to be done?	See section
1	Modification of hardware	PCS 7, step 1: Modification of hardware (Page 227)
2	Offline modification of the hardware configuration	PCS 7, Step 2: Offline modification of the hardware configuration (Page 228)
3	Stopping the standby CPU	PCS 7, Step 3: Stopping the standby CPU (Page 228)
4	Loading new hardware configuration in the standby CPU	PCS 7, Step 4: Loading new hardware configuration in the standby CPU (Page 229)
5	Switch to CPU with modified configuration	PCS 7, Step 5: Switch to CPU with modified configuration (Page 230)
6	Transition to redundant state	PCS 7, Step 6: Transition to redundant state (Page 231)
7	Editing and downloading the user program	PCS 7, Step 7: Editing and downloading the user program (Page 232)

Exceptions

This procedure for system modification does not apply in the following cases:

- To use free channels on an existing module
- For more information on adding interface modules (see section Adding interface modules in PCS 7 (Page 233))

Note

As of STEP 7 V5.3 SP2, after changing the hardware configuration, the load operation runs largely automatically. This means that you no longer need to perform the steps described in sections PCS 7, Step 3: Stopping the standby CPU (Page 228) to PCS 7, Step 6: Transition to redundant state (Page 231). The system behavior remains unchanged as already described.

You will find more information in the HW Config online help, "Download to module -> Download station configuration in RUN mode".

14.3.1 PCS 7, step 1: Modification of hardware

Starting situation

The fault-tolerant system is operating in redundant mode.

Procedure

1. Add the new components to the system.
   - Plug new central modules into the racks.
   - Plug new module into existing modular DP stations
   - Add new DP stations to existing DP master systems.

NOTICE
With switched I/O: Always complete all changes on **one** segment of the redundant DP master system before you modify the next segment.

2. Connect the required sensors and actuators to the new components.

Result

The insertion of non-configured modules will have no effect on the user program. The same applies to adding DP stations.

The fault-tolerant system is operating in redundant mode.

New components are not yet addressed.

14.3.2 PCS 7, Step 2: Offline modification of the hardware configuration

Starting situation

The fault-tolerant system is operating in redundant mode.

Procedure

1. Perform all the modifications to the hardware configuration relating to the added hardware offline. Assign appropriate icons to the new channels to be used.
2. Compile the new hardware configuration, but do **not** load it into the PLC just yet.

Result

The modified hardware configuration is in the PG/ES. The PLC continues operation with the old configuration in redundant mode.

Configuring connections

The interconnections with added CPs must be configured on both connection partners **after** you complete the HW modification.

14.3.3 PCS 7, Step 3: Stopping the standby CPU

Starting situation

The fault-tolerant system is operating in redundant mode.

Procedure

1. In SIMATIC Manager, select a CPU of the fault-tolerant system, then choose "PLC > Operating Mode" from the menu.
2. From the "Operating Mode" dialog box, select the standby CPU, then click "Stop".

Result

The standby CPU switches to STOP mode, the master CPU remains in RUN mode, the fault-tolerant system works in single mode. One-sided I/O of the standby CPU is no longer addressed.

Whilst I/O access errors of the one-sided I/O will result in OB 85 being called, due to the higher-priority CPU redundancy loss (OB 72) they will not be reported. OB 70 (I/O redundancy loss) is not called.

14.3.4 PCS 7, Step 4: Loading new hardware configuration in the standby CPU

Starting situation

The fault-tolerant system is operating in single mode.

Procedure

Load the compiled hardware configuration in the standby CPU that is in STOP mode.

NOTICE
The user program and connection configuration may not be downloaded in single mode.

Result

The new hardware configuration of the standby CPU does not yet have an effect on ongoing operation.

14.3.5 PCS 7, Step 5: Switch to CPU with modified configuration

Starting situation

The modified hardware configuration is loaded into the standby CPU.

Procedure

1. In SIMATIC Manager, select a CPU of the fault-tolerant system, then choose "PLC > Operating Mode" from the menu.
2. In the "Operating Mode" dialog box, click the "Switch to..." button.

In the "Switch" dialog box, select the "with altered configuration" option and click the "Switch" button.

1. Acknowledge the prompt for confirmation with "OK".

Result

The standby CPU links up, is updated (see section Link-up and update (Page 99)) and becomes the master. The previous master CPU switches to STOP mode, the fault-tolerant system operates with the new hardware configuration in single mode.

Reaction of the I/O

Type of I/O	One-sided I/O of previous master CPU	One-sided I/O of new master CPU	Switched I/O
Added I/O modules	are not addressed by the CPU.	are configured and updated by the CPU. Driver blocks are not yet present. Process or diagnostics interrupts are detected, but are not reported.	
I/O modules still present	are no longer addressed by the CPU. Output modules output the configured substitute or holding values.	are reconfigured [1] and updated by the CPU.	continue operation without interruption.
Added DP stations	are not addressed by the CPU.	as for added I/O modules (see above)	

[1] The central modules are first reset. Output modules briefly output 0 during this time (instead of the configured substitute or hold values).

Reaction to monitoring timeout

The update is aborted and no change of master takes place if one of the monitored times exceeds the configured maximum. The fault-tolerant system remains in single mode with the previous master CPU and in certain conditions attempts to perform the change of master later. For further information, refer to section Time monitoring (Page 114).

14.3.6 PCS 7, Step 6: Transition to redundant state

Starting situation

The fault-tolerant system is operating with the new hardware configuration in single mode.

Procedure

1. In SIMATIC Manager, select a CPU of the fault-tolerant system, then choose "PLC > Operating Mode" from the menu.
2. From the "Operating Mode" dialog box, select the standby CPU, then click "Warm Restart".

Result

The standby CPU links up and is updated. The fault-tolerant system is operating with the new hardware configuration in redundant mode.

Reaction of the I/O

Type of I/O	One-sided I/O of standby CPU	One-sided I/O of master CPU	Switched I/O
Added I/O modules	are configured and updated by the CPU. Driver blocks are not yet present. Any interrupts occurring are not reported.	are updated by the CPU. Driver blocks are not yet present. Process or diagnostics interrupts are detected, but are not reported.	
I/O modules still present	are reconfigured [1)] and updated by the CPU.	continue operation without interruption.	
Added DP stations	as for added I/O modules (see above)	Driver blocks are not yet present. Any interrupts occurring are not reported.	
1) Central modules are first reset. Output modules briefly output 0 during this time (instead of the configured substitute or hold values).			

Reaction to monitoring timeout

If one of the monitored times exceeds the configured maximum the update is aborted. The fault-tolerant system remains in single mode with the previous master CPU and in certain conditions attempts to perform the link-up and update later. For further information, refer to section Time monitoring (Page 114).

14.3.7 PCS 7, Step 7: Editing and downloading the user program

Starting situation

The fault-tolerant system is operating with the new hardware configuration in redundant mode.

> **CAUTION**
>
> The following program modifications are not possible in redundant state and result in the system mode Stop (both CPUs in STOP mode):
> - Structural modifications to an FB interface or the FB instance data.
> - Structural modifications to global DBs.
> - Compression of the CFC user program.
>
> Before the entire program is recompiled and reloaded due to such modifications the parameter values must be read back into the CFC, otherwise the modifications to the block parameters could be lost. You will find more detailed information on this topic in the *CFC for S7, Continuous Function Chart* manual.

Procedure

1. Adapt the program to the new hardware configuration. You can add the following components:
   – CFC and SFC charts
   – Blocks in existing charts
   – Connections and parameter settings
2. Assign parameters for the added channel drivers and interconnect them with the newly assigned icons (see section PCS 7, Step 2: Offline modification of the hardware configuration (Page 228)).
3. In SIMATIC Manager, select the charts folder and choose the "Options > Charts > Generate Module Drivers" menu command.
4. Compile only the modifications in the charts and load them into the PLC.

   > **NOTICE**
   >
   > Until an FC is called the first time, the value of its output is undefined. This must be taken into account in the interconnection of the FC outputs.

5. Configure the interconnections for the new CPs on both communication partners and download them to the PLC.

Result

The fault-tolerant system processes the entire system hardware with the new user program in redundant mode.

14.3.8 Adding interface modules in PCS 7

Always switch off the power before you install the IM460 and IM461 interface modules, external CP443-5 Extended DP master interface module and their connecting cables.

Always switch off power to an entire subsystem. To ensure that this does not influence the process, always set the subsystem to STOP before you do so.

Procedure

1. Change the hardware configuration offline (see section PCS 7, Step 2: Offline modification of the hardware configuration (Page 228))
2. Stop the standby CPU (see section PCS 7, Step 3: Stopping the standby CPU (Page 228))
3. Download the new hardware configuration to the standby CPU (see section PCS 7, Step 4: Loading new hardware configuration in the standby CPU (Page 229))
4. To expand the subsystem of the present standby CPU:
   - Switch off power to the standby subsystem.
   - Insert the new IM460 into the central unit and then establish the link to a new expansion unit.

     or
   - Add a new expansion unit to an existing chain.

     or
   - Plug in the new external DP master interface, and set up a new DP master system.
   - Switch on the power to the standby subsystem again.
5. Switch to the CPU with the modified configuration (see section PCS 7, Step 5: Switch to CPU with modified configuration (Page 230))
6. To expand the subsystem of the original master CPU (currently in STOP mode):
   - Switch off power to the standby subsystem.
   - Insert the new IM460 into the central unit and then establish the link to a new expansion unit.

     or
   - Add a new expansion unit to an existing chain.

     or
   - Plug in the new external DP master interface, and set up a new DP master system.
   - Switch on the power to the standby subsystem again.
7. Change to redundant mode (see section PCS 7, Step 6: Transition to redundant state (Page 231))
8. Modify and download the user program (see section PCS 7, Step 7: Editing and downloading the user program (Page 232))

14.4 Removing components in PCS 7

Starting situation

You have verified that the CPU parameters, such as monitoring times, match the planned new program. If they do not, adapt the CPU parameters first (see section Editing CPU parameters (Page 260)).

The modules to be removed and their connected sensors and actuators are no longer of any significance to the process being controlled. The fault-tolerant system is operating in redundant mode.

Procedure

Carry out the steps listed below to remove hardware components from a fault-tolerant system in PCS 7. Details of each step are listed in a subsection.

Step	What needs to be done?	See section
I	Offline modification of the hardware configuration	PCS 7, step I: Offline modification of the hardware configuration (Page 236)
II	Editing and downloading the user program	PCS 7, step II: Editing and downloading the user program (Page 237)
III	Stopping the standby CPU	PCS 7, step III: Stopping the standby CPU (Page 238)
IV	Loading new hardware configuration in the standby CPU	PCS 7, step IV: Loading new hardware configuration in the standby CPU (Page 238)
V	Switch to CPU with modified configuration	PCS 7, step V: Switch to CPU with modified configuration (Page 239)
VI	Transition to redundant state	PCS 7, step VI: Transition to redundant state (Page 240)
VII	Modification of hardware	PCS 7, step VII: Modification of hardware (Page 241)

Exceptions

This general procedure for system modifications does not apply to removing interface modules (see section Removing interface modules in PCS 7 (Page 242)).

Note

After changing the hardware configuration, it is downloaded practically automatically. This means that you no longer need to perform the steps described in sections PCS 7, step III: Stopping the standby CPU (Page 238) to PCS 7, step VI: Transition to redundant state (Page 240). The system behavior remains unchanged as already described.

You will find more information in the HW Config online help, "Download to module -> Download station configuration in RUN mode".

14.4.1 PCS 7, step I: Offline modification of the hardware configuration

Starting situation

The fault-tolerant system is operating in redundant mode.

Procedure

1. Perform offline only the configuration modifications relating to the hardware being removed. As you do, delete the icons to the channels that are no longer used.
2. Compile the new hardware configuration, but do **not** load it into the PLC just yet.

Result

The modified hardware configuration is in the PG/ES. The PLC continues operation with the old configuration in redundant mode.

14.4.2 PCS 7, step II: Editing and downloading the user program

Starting situation

The fault-tolerant system is operating in redundant mode.

CAUTION

The following program modifications are not possible in redundant state and result in the system mode Stop (both CPUs in STOP mode):

- Structural modifications to an FB interface or the FB instance data.
- Structural modifications to global DBs.
- Compression of the CFC user program.

Before the entire program is recompiled and reloaded due to such modifications the parameter values must be read back into the CFC, otherwise the modifications to the block parameters could be lost. You will find more detailed information on this topic in the *CFC for S7, Continuous Function Chart* manual.

Procedure

1. Only make program changes related to the hardware you are removing. You can delete the following components:
   – CFC and SFC charts
   – Blocks in existing charts
   – Channel drivers, interconnections and parameter settings
2. In SIMATIC Manager, select the charts folder and choose the "Options > Charts > Generate Module Drivers" menu command.

   This removes the driver blocks that are no longer required.
3. Compile only the modifications in the charts and download them to the PLC.

   NOTICE

   Until an FC is called the first time, the value of its output is undefined. This must be taken into account in the interconnection of the FC outputs.

Result

The fault-tolerant system continues to operate in redundant mode. The modified user program will no longer attempt to access the hardware being removed.

14.4.3 PCS 7, step III: Stopping the standby CPU

Starting situation

The fault-tolerant system is operating in redundant mode. The user program will no longer attempt to access the hardware being removed.

Procedure

1. In SIMATIC Manager, select a CPU of the fault-tolerant system, then choose "PLC > Operating Mode" from the menu.
2. From the "Operating Mode" dialog box, select the standby CPU, then click "Stop".

Result

The standby CPU switches to STOP mode, the master CPU remains in RUN mode, the fault-tolerant system works in single mode. One-sided I/O of the standby CPU is no longer addressed.

14.4.4 PCS 7, step IV: Loading new hardware configuration in the standby CPU

Starting situation

The fault-tolerant system is operating in single mode.

Procedure

Load the compiled hardware configuration in the standby CPU that is in STOP mode.

NOTICE
The user program and connection configuration can not be downloaded in single mode.

Result

The new hardware configuration of the standby CPU does not yet have an effect on ongoing operation.

14.4.5 PCS 7, step V: Switch to CPU with modified configuration

Starting situation

The modified hardware configuration is downloaded to the standby CPU.

Procedure

1. In SIMATIC Manager, select a CPU of the fault-tolerant system, then choose "PLC > Operating Mode" from the menu.
2. In the "Operating Mode" dialog box, click the "Switch to..." button.
3. In the "Switch" dialog box, select the "with altered configuration" option and click the "Switch" button.
4. Acknowledge the prompt for confirmation with "OK".

Result

The standby CPU links up, is updated (see section Link-up and update (Page 99)) and becomes the master. The previous master CPU switches to STOP mode, the fault-tolerant system operates with the new hardware configuration in single mode.

Reaction of the I/O

Type of I/O	One-sided I/O of previous master CPU	One-sided I/O of new master CPU	Switched I/O
I/O modules to be removed[1]	are no longer addressed by the CPU. Driver blocks are no longer present.		
I/O modules still present	are no longer addressed by the CPU. Output modules output the configured substitute or holding values.	are given new parameter settings[2] and updated by the CPU.	continue operation without interruption.
DP stations to be removed	as for I/O modules to be removed (see above)		
1) No longer included in the hardware configuration, but still plugged in 2) Central modules are first reset. Output modules briefly output 0 during this time (instead of the configured substitute or hold values).			

Reaction to monitoring timeout

The update is aborted and no change of master takes place if one of the monitored times exceeds the configured maximum. The fault-tolerant system remains in single mode with the previous master CPU and, assuming certain conditions are met, attempts the master changeover later. For further information, refer to section Time monitoring (Page 114).

14.4.6 PCS 7, step VI: Transition to redundant state

Starting situation

The fault-tolerant system is operating with the new hardware configuration in single mode.

Procedure

1. In SIMATIC Manager, select a CPU of the fault-tolerant system, then choose "PLC > Operating Mode" from the menu.
2. From the "Operating Mode" dialog box, select the standby CPU, then click "Warm Restart".

Result

The standby CPU links up and is updated. The fault-tolerant system is operating with the new hardware configuration in redundant mode.

Reaction of the I/O

Type of I/O	One-sided I/O of standby CPU	One-sided I/O of master CPU	Switched I/O
I/O modules to be removed[1)]	are no longer addressed by the CPU. Driver blocks are no longer present.		
I/O modules still present	are given new parameter settings[2)] and updated by the CPU.	continue operation without interruption.	
DP stations to be removed	as for I/O modules to be removed (see above)		

1) No longer included in the hardware configuration, but still plugged in

2) Central modules are first reset. Output modules briefly output 0 during this time (instead of the configured substitute or hold values).

Reaction to monitoring timeout

If one of the monitored times exceeds the configured maximum the update is aborted. The fault-tolerant system remains in single mode with the previous master CPU and, assuming certain conditions are met, attempts to the link-up and update later. For further information, refer to section Time monitoring (Page 114).

14.4.7 PCS 7, step VII: Modification of hardware

Starting situation

The fault-tolerant system is operating with the new hardware configuration in redundant mode.

Procedure

1. Disconnect all the sensors and actuators from the components you want to remove.
2. Unplug modules of the one-sided I/Os that are no longer required from the racks.
3. Unplug components that are no longer required from the modular DP stations.
4. Remove DP stations that are no longer required from the DP master systems.

NOTICE
With switched I/O: Always complete all changes on **one** segment of the redundant DP master system before you modify the next segment.

Result

The removal of non-configured modules does not influence the user program. The same applies to removing DP stations.

The fault-tolerant system is operating in redundant mode.

14.4.8 Removing interface modules in PCS 7

Always switch off the power before you remove the IM460 and IM461 interface modules, external CP 443-5 Extended DP master interface module and their connecting cables.

Always switch off power to an entire subsystem. To ensure that this does not influence the process, always set the subsystem to STOP before you do so.

Procedure

1. Change the hardware configuration offline (see section PCS 7, step I: Offline modification of the hardware configuration (Page 236))
2. Modify and download the user program (see section PCS 7, step II: Editing and downloading the user program (Page 237))
3. Stop the standby CPU (see section PCS 7, step III: Stopping the standby CPU (Page 238))
4. Download the new hardware configuration to the standby CPU (see section PCS 7, step IV: Loading new hardware configuration in the standby CPU (Page 238))
5. Follow the steps below to remove an interface module from the subsystem of the standby CPU:
   – Switch off power to the standby subsystem.
   – Remove an IM460 from the central unit.
     or
   – Remove an expansion unit from an existing chain.
     or
   – Remove an external DP master interface module.
   – Switch on the power to the standby subsystem again.
6. Switch to CPU with altered configuration (see section PCS 7, step V: Switch to CPU with modified configuration (Page 239))
7. To remove an interface module from the subsystem of the original master CPU (currently in STOP mode):
   – Switch off power to the standby subsystem.
   – Remove an IM460 from the central unit.
     or
   – Remove an expansion unit from an existing chain.
     or
   – Remove an external DP master interface module.
   – Switch on the power to the standby subsystem again.
8. Change to redundant mode (see section PCS 7, step VI: Transition to redundant state (Page 240))

14.5 Adding components in STEP 7

Starting situation

You have verified that the CPU parameters, such as monitoring times, match the planned new program. If they do not, adapt the CPU parameters first (see section Editing CPU parameters (Page 260)).

The fault-tolerant system is operating in redundant mode.

Procedure

Carry out the steps listed below to add hardware components to a fault-tolerant system in STEP 7. Details of each step are listed in a subsection.

Step	What has to be done?	See section
1	Modification of hardware	STEP 7, step 1: Adding hardware (Page 245)
2	Offline modification of the hardware configuration	STEP 7, step 2: Offline modification of the hardware configuration (Page 246)
3	Expanding and downloading OBs	STEP 7, step 3: Expanding and downloading OBs (Page 246)
4	Stopping the standby CPU	STEP 7, step 4: Stopping the standby CPU (Page 247)
5	Loading new hardware configuration in the standby CPU	STEP 7, step 5: Loading new hardware configuration in the standby CPU (Page 247)
6	Switch to CPU with altered configuration	STEP 7, step 6: Switch to CPU with modified configuration (Page 248)
7	Change to redundant mode	STEP 7, step 7: Transition to redundant state (Page 249)
8	Editing and downloading the user program	STEP 7, step 8: Editing and downloading the user program (Page 250)

Exceptions

This procedure for system modification does not apply in the following cases:

- To use free channels on an existing module
- For more information on adding interface modules (see section Adding interface modules in STEP 7 (Page 251))

Note

After changing the hardware configuration, it is downloaded practically automatically. This means that you no longer need to perform the steps described in sections STEP 7, step 4: Stopping the standby CPU (Page 247) to STEP 7, step 8: Editing and downloading the user program (Page 250). The system behavior remains unchanged as already described.

You will find more information in the HW Config online help, "Download to module -> Download station configuration in RUN mode".

14.5.1 STEP 7, Stepp 1: Adding hardware

Starting situation

The fault-tolerant system is operating in redundant mode.

Procedure

1. Add the new components to the system.
   – Plug new central modules into the racks.
   – Plug new module into existing modular DP stations
   – Add new DP stations to existing DP master systems.

NOTICE
With switched I/O: Always complete all changes on **one** segment of the redundant DP master system before you modify the next segment.

2. Connect the required sensors and actuators to the new components.

Result

The insertion of non-configured modules will have no effect on the user program. The same applies to adding DP stations.

The fault-tolerant system is operating in redundant mode.

New components are not yet addressed.

14.5.2 STEP 7, step 2: Offline modification of the hardware configuration

Starting situation

The fault-tolerant system is operating in redundant mode. The modules added are not yet addressed.

Procedure

1. Perform all the modifications to the hardware configuration relating to the added hardware offline.
2. Compile the new hardware configuration, but do **not** load it into the PLC just yet.

Result

The modified hardware configuration is in the PG. The PLC continues operation with the old configuration in redundant mode.

Configuring connections

The interconnections with added CPs must be configured on both connection partners **after** you complete the HW modification.

14.5.3 STEP 7, step 3: Expanding and downloading OBs

Starting situation

The fault-tolerant system is operating in redundant mode.

Procedure

1. Verify that the interrupt OBs 4x, 82, 83, 85, 86, OB88 and 122 react to any interrupts of the new components as intended.
2. Download the modified OBs and the corresponding program elements to the PLC.

Result

The fault-tolerant system is operating in redundant mode.

14.5.4 STEP 7, step 4: Stopping the standby CPU

Starting situation

The fault-tolerant system is operating in redundant mode.

Procedure

1. In SIMATIC Manager, select a CPU of the fault-tolerant system, then choose "PLC > Operating Mode" from the menu.
2. From the "Operating Mode" dialog box, select the standby CPU, then click "Stop".

Result

The standby CPU switches to STOP mode, the master CPU remains in RUN mode, the fault-tolerant system works in single mode. One-sided I/O of the standby CPU is no longer addressed. OB 70 (I/O redundancy loss) is not called due to the higher-priority CPU redundancy loss (OB72).

14.5.5 STEP 7, step 5: Loading new hardware configuration in the standby CPU

Starting situation

The fault-tolerant system is operating in single mode.

Procedure

Load the compiled hardware configuration in the standby CPU that is in STOP mode.

NOTICE
The user program and connection configuration can not be downloaded in single mode.

Result

The new hardware configuration of the standby CPU does not yet have an effect on ongoing operation.

14.5.6 STEP 7, step 6: Switch to CPU with modified configuration

Starting situation

The modified hardware configuration is downloaded to the standby CPU.

Procedure

1. In SIMATIC Manager, select a CPU of the fault-tolerant system, then choose "PLC > Operating Mode" from the menu.
2. In the "Operating Mode" dialog box, click the "Switch to..." button.
3. In the "Switch" dialog box, select the "with altered configuration" option and click the "Switch" button.
4. Acknowledge the prompt for confirmation with "OK".

Result

The standby CPU links up, is updated and becomes the master. The previous master CPU switches to STOP mode, the fault-tolerant system operates with the new hardware configuration in single mode.

Reaction of the I/O

Type of I/O	One-sided I/O of previous master CPU	One-sided I/O of new master CPU	Switched I/O
Added I/O modules	are not addressed by the CPU.	are given new parameter settings and updated by the CPU. The output modules temporarily output the configured substitution values.	
I/O modules still present	are no longer addressed by the CPU. Output modules output the configured substitute or holding values.	are given new parameter settings[1] and updated by the CPU.	continue operation without interruption.
Added DP stations	are not addressed by the CPU.	as for added I/O modules (see above)	
1) Central modules are first reset. Output modules briefly output 0 during this time (instead of the configured substitute or hold values).			

Reaction to monitoring timeout

The update is aborted and no change of master takes place if one of the monitored times exceeds the configured maximum. The fault-tolerant system remains in single mode with the previous master CPU and, assuming certain conditions are met, attempts the master changeover later. For further information, refer to section Time monitoring (Page 114).

14.5.7 STEP 7, step 7: Transition to redundant state

Starting situation

The fault-tolerant system is operating with the new hardware configuration in single mode.

Procedure

1. In SIMATIC Manager, select a CPU of the fault-tolerant system, then choose "PLC > Operating Mode" from the menu.
2. From the "Operating Mode" dialog box, select the standby CPU, then click "Warm Restart".

Result

The standby CPU links up and is updated. The fault-tolerant system is operating with the new hardware configuration in redundant mode.

Reaction of the I/O

Type of I/O	One-sided I/O of standby CPU	One-sided I/O of master CPU	Switched I/O
Added I/O modules	are given new parameter settings and updated by the CPU. The output modules temporarily output the configured substitution values.	are updated by the CPU.	are updated by the CPU. Generate insertion interrupt; must be ignored in OB83.
I/O modules still present	are given new parameter settings[1)] and updated by the CPU.	continue operation without interruption.	
Added DP stations	as for added I/O modules (see above)	are updated by the CPU.	
1) Central modules are first reset. Output modules briefly output 0 during this time (instead of the configured substitute or hold values).			

Reaction to monitoring timeout

If one of the monitored times exceeds the configured maximum the update is aborted. The fault-tolerant system remains in single mode with the previous master CPU and, assuming certain conditions are met, attempts to the link-up and update later. For further information, refer to section Time monitoring (Page 114).

14.5.8 STEP 7, step 8: Editing and downloading the user program

Starting situation

The fault-tolerant system is operating with the new hardware configuration in redundant mode.

Restrictions

CAUTION
Any attempts to modify the structure of an FB interface or the instance data of an FB in redundant mode will lead to a system STOP at both CPUs.

Procedure

1. Adapt the program to the new hardware configuration.

   You can add, edit or remove OBs, FBs, FCs and DBs.
2. Download only the program changes to the PLC.
3. Configure the interconnections for the new CPs on both communication partners and download them to the PLC.

Result

The fault-tolerant system processes the entire system hardware with the new user program in redundant mode.

14.5.9 Adding interface modules in STEP 7

Always switch off the power before you install the IM460 and IM461 interface modules, external CP443-5 Extended DP master interface module and their connecting cables.

Always switch off power to an entire subsystem. To ensure that this does not influence the process, always set the subsystem to STOP before you do so.

Procedure

1. Change the hardware configuration offline (see section STEP 7, step 2: Offline modification of the hardware configuration (Page 246))
2. Expand and download the organization blocks (see section STEP 7, step 3: Expanding and downloading OBs (Page 246))
3. Stop the standby CPU (see section STEP 7, step 4: Stopping the standby CPU (Page 247))
4. Download the new hardware configuration to the standby CPU (see section STEP 7, step 5: Loading new hardware configuration in the standby CPU (Page 247))
5. To expand the subsystem of the present standby CPU:
   - Switch off power to the standby subsystem.
   - Insert the new IM460 into the central unit and then establish the link to a new expansion unit.

     or
   - Add a new expansion unit to an existing chain.

     or
   - Plug in the new external DP master interface, and install a new DP master system.
   - Switch on the power to the standby subsystem again.
6. Switch to CPU with altered configuration (see section STEP 7, step 6: Switch to CPU with modified configuration (Page 248))
7. To expand the subsystem of the original master CPU (currently in STOP mode):
   - Switch off power to the standby subsystem.
   - Insert the new IM460 into the central unit, then establish the link to a new expansion unit.

     or
   - Add a new expansion unit to an existing chain.

     or
   - Plug in the new external DP master interface, and install a new DP master system.
   - Switch on the power to the standby subsystem again.
8. Change to redundant mode (see section STEP 7, step 7: Transition to redundant state (Page 249))
9. Modify and download the user program (see section STEP 7, step 8: Editing and downloading the user program (Page 250))

14.6 Removing components in STEP 7

Starting situation

You have verified that the CPU parameters, such as monitoring times, match the planned new program. If they do not, adapt the CPU parameters first (see section Editing CPU parameters (Page 260)).

The modules to be removed and their connected sensors and actuators are no longer of any significance to the process being controlled. The fault-tolerant system is operating in redundant mode.

Procedure

Carry out the steps listed below to remove hardware components from a fault-tolerant system in STEP 7. Details of each step are listed in a subsection.

Step	What has to be done?	See section
I	Offline modification of the hardware configuration	STEP 7, step I: Offline modification of the hardware configuration (Page 253)
II	Editing and downloading the user program	STEP 7, step II: Editing and downloading the user program (Page 254)
III	Stopping the standby CPU	STEP 7, step III: Stopping the standby CPU (Page 254)
IV	Loading new hardware configuration in the standby CPU	STEP 7, step IV: Loading new hardware configuration in the standby CPU (Page 255)
V	Switch to CPU with altered configuration	STEP 7, step V: Switch to CPU with modified configuration (Page 256)
VI	Change to redundant mode	STEP 7, step VI: Transition to redundant state (Page 257)
VII	Modification of hardware	STEP 7, step VII: Modification of hardware (Page 258)
VIII	Editing and downloading organization blocks	STEP 7, step VIII: Editing and downloading organization blocks (Page 258)

Exceptions

This general procedure for system modifications does not apply to removing interface modules (see section Removing interface modules in STEP 7 (Page 259)).

Note

After changing the hardware configuration, it is downloaded practically automatically. This means that you no longer need to perform the steps described in sections STEP 7, step III: Stopping the standby CPU (Page 254) to STEP 7, step VI: Transition to redundant state (Page 257). The system behavior remains unchanged as already described.

You will find more information in the HW Config online help, "Download to module -> Download station configuration in RUN mode".

14.6.1 STEP 7, step I: Offline modification of the hardware configuration

Starting situation

The fault-tolerant system is operating in redundant mode.

Procedure

1. Perform all the modifications to the hardware configuration relating to the hardware being removed offline.
2. Compile the new hardware configuration, but do **not** load it into the PLC just yet.

Result

The modified hardware configuration is in the PG. The PLC continues operation with the old configuration in redundant mode.

14.6.2 STEP 7, step II: Editing and downloading the user program

Starting situation

The fault-tolerant system is operating in redundant mode.

Restrictions

> **CAUTION**
>
> Any attempts to modify the structure of an FB interface or the instance data of an FB in redundant mode will lead to a system STOP at both CPUs.

Procedure

1. Edit only the program elements related to the hardware removal.

   You can add, edit or remove OBs, FBs, FCs and DBs.
2. Download only the program changes to the PLC.

Result

The fault-tolerant system is operating in redundant mode. The new user program will no longer attempt to access the hardware being removed.

14.6.3 STEP 7, step III: Stopping the standby CPU

Starting situation

The fault-tolerant system is operating in redundant mode. The user program will no longer attempt to access the hardware being removed.

Procedure

1. In SIMATIC Manager, select a CPU of the fault-tolerant system, then choose "PLC > Operating Mode" from the menu.
2. From the "Operating Mode" dialog box, select the standby CPU, then click "Stop".

Result

The standby CPU switches to STOP mode, the master CPU remains in RUN mode, the fault-tolerant system works in single mode. One-sided I/O of the standby CPU is no longer addressed.

14.6.4 STEP 7, step IV: Loading new hardware configuration in the standby CPU

Starting situation

The fault-tolerant system is operating in single mode.

Procedure

Load the compiled hardware configuration in the standby CPU that is in STOP mode.

NOTICE
The user program and connection configuration can not be downloaded in single mode.

Result

The new hardware configuration of the standby CPU does not yet have an effect on ongoing operation.

14.6.5 STEP 7, step V: Switch to CPU with modified configuration

Starting situation

The modified hardware configuration is downloaded to the standby CPU.

Procedure

1. In SIMATIC Manager, select a CPU of the fault-tolerant system, then choose "PLC > Operating Mode" from the menu.
2. In the "Operating Mode" dialog box, click the "Switch to..." button.
3. In the "Switch" dialog box, select the "with altered configuration" option and click the "Switch" button.
4. Acknowledge the prompt for confirmation with "OK".

Result

The standby CPU links up, is updated (see section Link-up and update (Page 99)) and becomes the master. The previous master CPU switches to STOP mode, the fault-tolerant system continues operating in single mode.

Reaction of the I/O

Type of I/O	One-sided I/O of previous master CPU	One-sided I/O of new master CPU	Switched I/O
I/O modules to be removed1)	are no longer addressed by the CPU.		
I/O modules still present	are no longer addressed by the CPU. Output modules output the configured substitute or holding values.	are given new parameter settings2) and updated by the CPU.	continue operation without interruption.
DP stations to be removed	as for I/O modules to be removed (see above)		
1) No longer included in the hardware configuration, but still plugged in 2) Central modules are first reset. Output modules briefly output 0 during this time (instead of the configured substitute or hold values).			

Reaction to monitoring timeout

The update is aborted and no change of master takes place if one of the monitored times exceeds the configured maximum. The fault-tolerant system remains in single mode with the previous master CPU and, assuming certain conditions are met, attempts the master changeover later. For further information, refer to section Time monitoring (Page 114).

14.6.6 STEP 7, step VI: Transition to redundant state

Starting situation

The fault-tolerant system is operating with the new (restricted) hardware configuration in single mode.

Procedure

1. In SIMATIC Manager, select a CPU of the fault-tolerant system, then choose "PLC > Operating Mode" from the menu.
2. From the "Operating Mode" dialog box, select the standby CPU, then click "Warm Restart".

Result

The standby CPU links up and is updated. The fault-tolerant system is operating in redundant mode.

Reaction of the I/O

<table>
<tr><th>Type of I/O</th><th>One-sided I/O of standby CPU</th><th>One-sided I/O of master CPU</th><th>Switched I/O</th></tr>
<tr><td>I/O modules to be removed[1]</td><td colspan="3">are no longer addressed by the CPU.</td></tr>
<tr><td>I/O modules still present</td><td>are given new parameter settings[2] and updated by the CPU.</td><td colspan="2">continue operation without interruption.</td></tr>
<tr><td>DP stations to be removed</td><td colspan="3">as for I/O modules to be removed (see above)</td></tr>
<tr><td colspan="4">1) No longer included in the hardware configuration, but still plugged in
2) Central modules are first reset. Output modules briefly output 0 during this time (instead of the configured substitute or hold values).</td></tr>
</table>

Reaction to monitoring timeout

If one of the monitored times exceeds the configured maximum the update is aborted. The fault-tolerant system remains in single mode with the previous master CPU and, assuming certain conditions are met, attempts to the link-up and update later. For further information, refer to section Time monitoring (Page 114).

14.6.7 STEP 7, step VII: Modification of hardware

Starting situation

The fault-tolerant system is operating with the new hardware configuration in redundant mode.

Procedure

1. Disconnect all the sensors and actuators from the components you want to remove.
2. Remove the relevant components from the system.
   – Remove the central modules from the rack.
   – Remove the modules from modular DP stations
   – Remove DP stations from DP master systems.

NOTICE
With switched I/O: Always complete all changes on **one** segment of the redundant DP master system before you modify the next segment.

Result

The removal of non-configured modules does not influence the user program. The same applies to removing DP stations.

The fault-tolerant system is operating in redundant mode.

14.6.8 STEP 7, step VIII: Editing and downloading organization blocks

Starting situation

The fault-tolerant system is operating in redundant mode.

Procedure

1. Make sure that the interrupt OBs 4x and 82 no longer contain any interrupts of the removed components.
2. Download the modified OBs and the corresponding program elements to the PLC.

Result

The fault-tolerant system is operating in redundant mode.

14.6.9 Removing interface modules in STEP 7

Always switch off the power before you remove the IM460 and IM461 interface modules, external CP 443-5 Extended DP master interface module and their connecting cables.

Always switch off power to an entire subsystem. To ensure that this does not influence the process, always set the subsystem to STOP before you do so.

Procedure

1. Change the hardware configuration offline (see section STEP 7, step I: Offline modification of the hardware configuration (Page 253))
2. Modify and download the user program (see section STEP 7, step II: Editing and downloading the user program (Page 254))
3. Stop the standby CPU (see section STEP 7, step III: Stopping the standby CPU (Page 254))
4. Download the new hardware configuration to the standby CPU (see section STEP 7, step IV: Loading new hardware configuration in the standby CPU (Page 255))
5. Follow the steps below to remove an interface module from the subsystem of the standby CPU:
   – Switch off power to the standby subsystem.
   – Remove an IM460 from the central unit.
     or
   – Remove an expansion unit from an existing chain.
     or
   – Remove an external DP master interface module.
   – Switch on the power to the standby subsystem again.
6. Switch to CPU with altered configuration (see section STEP 7, step V: Switch to CPU with modified configuration (Page 256))
7. To remove an interface module from the subsystem of the original master CPU (currently in STOP mode):
   – Switch off power to the standby subsystem.
   – Remove an IM460 from the central unit.
     or
   – Remove an expansion unit from an existing chain.
     or
   – Remove an external DP master interface module.
   – Switch on the power to the standby subsystem again.
8. Change to redundant mode (see section STEP 7, step VI: Transition to redundant state (Page 257))
9. Modify and download the user organization blocks (see section STEP 7, step VIII: Editing and downloading organization blocks (Page 258))

14.7 Editing CPU parameters

14.7.1 Editing CPU parameters

Only certain CPU parameters (object properties) can be edited in operation. These are highlighted on the screen forms by blue text. If you have set blue as the color for dialog box text on the Windows Control Panel, the editable parameters are indicated in black characters.

NOTICE
If you edit any protected parameters, the system will reject any attempt to changeover to the CPU containing those modified parameters. The error event W#16#5966 is triggered and written to the diagnostic buffer, and you will then have to restore the wrongly changed parameters in the parameter configuration to their last valid values.

Table 14-1 Modifiable CPU parameters

Tab	Editable parameter
Startup	Monitoring time for signaling readiness by modules
	Monitoring time for transferring parameters to modules
Cycle/clock memory	Cycle monitoring time
	Cycle load due to communication
	Size of the process image of inputs *)
	Size of the process image of outputs *)
Memory	Local data for the various priority classes *)
	Communication resources: Maximum number of communication requests .You may only increase the configured value of this parameter. *).
Time-of-day interrupts (for each time-of-day interrupt OB)	"Active" checkbox
	"Execution" list box
	Starting date
	Time
Cyclic interrupt (for each cyclic interrupt OB)	Execution
	Phase offset
Diagnostics/clock	Correction factor
Security	Protection level and password
H parameter	Test cycle time
	Maximum cycle time extension
	Maximum communication delay
	Maximum inhibit time for priority classes > 15
	Minimum I/O retention time
*) Modifying these parameters also modifies the memory content.	

The selected new values should match both the currently loaded and the planned new user program.

Starting situation

The fault-tolerant system is operating in redundant mode.

Procedure

To edit the CPU parameters of a fault-tolerant system, follow the steps outlined below. Details of each step are listed in a subsection.

Step	What has to be done?	See section
A	Editing CPU parameters offline	Step A: Editing CPU parameters offline (Page 262)
B	Stopping the standby CPU	Step B: Stopping the standby CPU (Page 262)
C	Downloading modified CPU parameters to the standby CPU	Step C: Loading new hardware configuration in the standby CPU (Page 263)
D	Switch to CPU with altered configuration	Step D: Switch to CPU with modified configuration (Page 264)
E	Change to redundant mode	Step E: Transition to redundant state (Page 265)

Note

After changing the hardware configuration, it is downloaded practically automatically. This means that you no longer need to perform the steps described in sections Step B: Stopping the standby CPU (Page 262) to Step E: Transition to redundant state (Page 265). The system behavior remains unchanged as already described.

You will find more information in the HW Config online help, "Download to module -> Download station configuration in RUN mode". You will find more information in the HW Config online help, "Download to module -> Download station configuration in RUN mode".

14.7.2 Step A: Editing CPU parameters offline

Starting situation

The fault-tolerant system is operating in redundant mode.

Procedure

1. Edit the relevant CPU properties offline in HW Config.
2. Compile the new hardware configuration, but do **not** load it into the PLC just yet.

Result

The modified hardware configuration is in the PG/ES. The PLC continues operation with the old configuration in redundant mode.

14.7.3 Step B: Stopping the standby CPU

Starting situation

The fault-tolerant system is operating in redundant mode.

Procedure

1. In SIMATIC Manager, select a CPU of the fault-tolerant system, then choose "PLC > Operating Mode" from the menu.
2. From the "Operating Mode" dialog box, select the standby CPU, then click "Stop".

Result

The standby CPU switches to STOP mode, the master CPU remains in RUN mode, the fault-tolerant system works in single mode. One-sided I/O of the standby CPU is no longer addressed.

14.7.4 Step C: Loading new hardware configuration in the standby CPU

Starting situation

The fault-tolerant system is operating in single mode.

Procedure

Load the compiled hardware configuration in the standby CPU that is in STOP mode.

NOTICE
The user program and connection configuration can not be downloaded in single mode.

Result

The modified CPU parameters in the new hardware configuration of the standby CPU do not yet have an effect on ongoing operation.

14.7.5 Step D: Switch to CPU with modified configuration

Starting situation

The modified hardware configuration is downloaded to the standby CPU.

Procedure

1. In SIMATIC Manager, select a CPU of the fault-tolerant system, then choose "PLC > Operating Mode" from the menu.
2. In the "Operating Mode" dialog box, click the "Switch to..." button.
3. In the "Switch" dialog box, select the "with altered configuration" option and click the "Switch" button.
4. Acknowledge the prompt for confirmation with "OK".

Result

The standby CPU links up, is updated and becomes the master. The previous master CPU switches to STOP mode, the fault-tolerant system continues operating in single mode.

Reaction of the I/O

Type of I/O	One-sided I/O of previous master CPU	One-sided I/O of new master CPU	Switched I/O
I/O modules	are no longer addressed by the CPU. Output modules output the configured substitute or holding values.	are given new parameter settings1) and updated by the CPU.	continue operation without interruption.
1) Central modules are first reset. Output modules briefly output 0 during this time (instead of the configured substitute or hold values).			

Reaction to monitoring timeout

The update is aborted and no change of master takes place if one of the monitored times exceeds the configured maximum. The fault-tolerant system remains in single mode with the previous master CPU and, assuming certain conditions are met, attempts the master changeover later. For further information, refer to section Time monitoring (Page 114).

Where the values for the monitoring times in the CPUs differ, the higher values always apply.

14.7.6 Step E: Transition to redundant state

Starting situation

The fault-tolerant system operates with the modified CPU parameters in single mode.

Procedure

1. In SIMATIC Manager, select a CPU of the fault-tolerant system, then choose "PLC > Operating Mode" from the menu.
2. From the "Operating Mode" dialog box, select the standby CPU, then click "Warm Restart".

Result

The standby CPU links up and is updated. The fault-tolerant system is operating in redundant mode.

Reaction of the I/O

Type of I/O	One-sided I/O of standby CPU	One-sided I/O of master CPU	Switched I/O
I/O modules	are given new parameter settings[1)] and updated by the CPU.	continue operation without interruption.	
1) Central modules are first reset. Output modules briefly output 0 during this time (instead of the configured substitute or hold values).			

Reaction to monitoring timeout

If one of the monitored times exceeds the configured maximum the update is aborted. The fault-tolerant system remains in single mode with the previous master CPU and, assuming certain conditions are met, attempts to the link-up and update later. For further information, refer to section Time monitoring (Page 114).

Where the values for the monitoring times in the CPUs differ, the higher values always apply.

14.8 Changing the CPU memory configuration

14.8.1 Changing the CPU memory configuration

The redundant system state is only possible if both CPUs have the same memory configuration. For this the following condition must be met:

- The size and type of load memory (RAM or FLASH) on both CPUs must match.

The memory configuration of the CPUs can be modified in operation. Possible modifications of S7-400H memory :

- Expanding load memory
- Changing the type of load memory

14.8.2 Expanding load memory

The following methods of memory expansion are possible:

- Upgrade the load memory by inserting a memory card with more memory space
- Upgrade the load memory by inserting a RAM card, if no memory card was previously inserted

If you change memory in this way, the entire user program is copied from the master CPU to the standby CPU during the link-up process (see section Update sequence (Page 107)).

Restrictions

Memory should preferably be expanded using RAM cards, because this will ensure that the user program is copied to load memory of the standby CPU in the link-up process.

In principle, it is also feasible to use FLASH cards to expand load memory. However, you will then have to explicitly download the entire user program and the hardware configuration to the new FLASH card (see procedure in section Changing the type of load memory (Page 268)).

Starting situation

The fault-tolerant system is operating in redundant mode.

Procedure

Do the following in the sequence given:

Step	What has to be done?	How does the system react?
1	Switch the standby CPU to STOP using the PG.	The system is now operating in single mode.
2	Replace the memory card in the CPU with a card which has a higher capacity as required.	Standby CPU requests memory reset.
3	Reset the standby CPU using the PG.	–
4	Start the standby CPU with the menu command "PLC > Mode > Switch to CPU ... with expanded memory configuration".	• The standby CPU links up, is updated and becomes the master. • Previous master CPU changes to STOP. • System operates in single mode.
5	Turn off power to the second CPU.	The subsystem is disabled.
6	Modify the memory configuration of the second CPU as you did in steps 2 to 3 for the first CPU.	–
7	Start the second CPU from the PG.	• The second CPU is linked up and updated. • The system is now operating again in redundant mode.

14.8.3 Changing the type of load memory

The following types of memory cards are available for load memory:

- RAM card for the test and commissioning phase
- FLASH card for permanent storage of the completed user program

The size of the new memory card is irrelevant here.

If you change your memory configuration in this way, the system does not transfer any program elements from the master CPU to the standby CPU. Instead, it transfers only the contents of the unchanged blocks of the user program (see section Switch to CPU with modified configuration or expanded memory configuration (Page 110)).

It is the user's responsibility to download the entire user program to the new load memory.

Starting situation

The fault-tolerant system is operating in redundant mode.

The current status of the user program is available on the PG/ES as a STEP 7 project in block format.

CAUTION
You can not deploy a user program you uploaded from the PLC here. It is not permissible to recompile the user program from an STL source file, because this action would set a new time stamp at all blocks and so prevent the block contents from being copied when you change over the master/standby station.

Procedure

Do the following in the sequence given:

Step	What has to be done?	How does the system react?
1	Switch the standby CPU to STOP using the PG.	The system is now operating in single mode.
2	Replace the existing memory card in the standby CPU with a new one of the required type.	Standby CPU requests memory reset.
3	Reset the standby CPU using the PG.	–
4	Download the program data to the standby CPU in STEP 7 by selecting the "Download User Program to Memory Card" command. **Notice**: Select the correct CPU from the selection dialog.	–
5	Start the standby CPU with the menu command "PLC > Mode > Switch to CPU ... with altered configuration".	• The standby CPU links up, is updated and becomes the master. • Previous master CPU changes to STOP. • System operates in single mode.
6	Modify the memory configuration of the second CPU as you did for the first CPU in step 2.	–
7	Download the user program and the hardware configuration to the second CPU.	–
8	Start the second CPU from the PG.	• The second CPU is linked up and updated. • The system is now operating again in redundant mode.

NOTICE

If you want to change to FLASH cards, you can load them with the user program and hardware configuration in advance without inserting them in the CPU. Steps 4 and 7 can then be omitted.

However, the memory cards in both CPUs must be loaded in the same sequence. Changing the order of blocks in the load memories will lead to a link-up abort.

Writing to a FLASH card in the fault-tolerant system

You can always write to a FLASH card while the fault-tolerant system is in RUN, without having to stop the fault-tolerant system. This is, however, only possible if the online data of the hardware configuration and the user program in both CPUs and the corresponding offline data in your engineering station match.

Follow the steps outlined below:

1. Set the standby CPU to STOP and insert the FLASH card into the CPU.
2. Run a CPU memory reset using STEP 7.
3. Download the hardware configuration using STEP 7.
4. Download the program data with the STEP 7 "Download User Program to Memory Card" command. Notice: Select the correct CPU from the selection dialog.
5. Switch to the CPU with the changed configuration using the "Operating Mode" dialog. This changes over the master/standby roles; the CPU with the flash card is now the master CPU. The standby CPU is now in STOP.
6. Next, insert the flash card in the CPU that is in STOP. Run a CPU memory reset using STEP 7.
7. Carry out step 4: Download the program data with the STEP 7 "Download User Program to Memory Card" command. Notice: Select the correct CPU from the selection dialog.
8. Run a warm restart on the standby CPU using the "Operating Mode" dialog. The system status now changes to "Redundant" mode.

The online and offline data consistency described earlier also applies when you remove FLASH cards from a fault-tolerant system. In addition, the available RAM size must not be less than the actual size of the STEP 7 program (STEP 7 Program > Block Container > Properties "Blocks").

1. Set the standby CPU to STOP and remove the FLASH card. Adapt the memory configuration as required.
2. Run a CPU memory reset using STEP 7.
3. Download the block container using STEP 7.
4. Switch to the CPU with the changed configuration using the "Operating Mode" dialog.
5. Remove the FLASH card from the CPU which is now in STOP. Adapt the RAM configuration as required, and then perform a CPU memory reset.
6. Run a warm restart on the standby CPU using the "Operating Mode" dialog. The system status now changes to "Redundant" mode.

14.9 Reconfiguration of a module

14.9.1 Reconfiguration of a module

Refer to the information text in the "Hardware Catalog" window to determine which modules (signal modules and function modules) can be reconfigured during ongoing operation. The specific reactions of individual modules are described in the respective technical documentation.

NOTICE
If you edit any protected parameters, the system will reject any attempt to changeover to the CPU containing those modified parameters. The error event W#16#5966 is triggered and written to the diagnostic buffer, and you will then have to restore the wrongly changed parameters in the parameter configuration to their last valid values.

The selected new values must match the current and the planned user program.

Starting situation

The fault-tolerant system is operating in redundant mode.

Procedure

To edit the parameters of modules in a fault-tolerant system, perform the steps outlined below. Details of each step are listed in a subsection.

Step	What has to be done?	See section
A	Editing parameters offline	Step A: Editing parameters offline (Page 273)
B	Stopping the standby CPU	Step B: Stopping the standby CPU (Page 274)
C	Downloading modified CPU parameters to the standby CPU	Step C: Loading new hardware configuration in the standby CPU (Page 274)
D	Switch to CPU with altered configuration	Step D: Switch to CPU with modified configuration (Page 275)
E	Change to redundant mode	Step E: Transition to redundant state (Page 277)

Note

After changing the hardware configuration, it is downloaded practically automatically. This means that you no longer need to perform the steps described in sections Step B: Stopping the standby CPU (Page 274) to Step E: Transition to redundant state (Page 277). The system behavior remains unchanged as already described.

You will find more information in the HW Config online help, "Download to module -> Download station configuration in RUN mode".

14.9.2 Step A: Editing parameters offline

Starting situation

The fault-tolerant system is operating in redundant mode.

Procedure

1. Edit the module parameters offline in HW Config.
2. Compile the new hardware configuration, but do **not** load it into the PLC just yet.

Result

The modified hardware configuration is in the PG/ES. The PLC continues operation with the old configuration in redundant mode.

14.9.3 Step B: Stopping the standby CPU

Starting situation

The fault-tolerant system is operating in redundant mode.

Procedure

1. In SIMATIC Manager, select a CPU of the fault-tolerant system, then choose "PLC > Operating Mode" from the menu.
2. From the "Operating Mode" dialog box, select the standby CPU, then click "Stop".

Result

The standby CPU switches to STOP mode, the master CPU remains in RUN mode, the fault-tolerant system works in single mode. One-sided I/O of the standby CPU is no longer addressed.

14.9.4 Step C: Loading new hardware configuration in the standby CPU

Starting situation

The fault-tolerant system is operating in single mode.

Procedure

Load the compiled hardware configuration in the standby CPU that is in STOP mode.

NOTICE
The user program and connection configuration can not be downloaded in single mode.

Result

The modified parameters in the new hardware configuration of the standby CPU do not yet have an effect on ongoing operation.

14.9.5 Step D: Switch to CPU with modified configuration

Starting situation

The modified hardware configuration is downloaded to the standby CPU.

Procedure

1. In SIMATIC Manager, select a CPU of the fault-tolerant system, then choose "PLC > Operating Mode" from the menu.
2. In the "Operating Mode" dialog box, click the "Switch to..." button.
3. In the "Switch" dialog box, select the "with altered configuration" option and click the "Switch" button.
4. Acknowledge the prompt for confirmation with "OK".

Result

The standby CPU links up, is updated and becomes the master. The previous master CPU switches to STOP mode, the fault-tolerant system continues operating in single mode.

Reaction of the I/O

Type of I/O	One-sided I/O of previous master CPU	One-sided I/O of new master CPU	Switched I/O
I/O modules	are no longer addressed by the CPU. Output modules output the configured substitute or holding values.	are given new parameter settings1) and updated by the CPU.	continue operation without interruption.
1) Central modules are first reset. Output modules briefly output 0 during this time (instead of the configured substitute or hold values).			

Reaction to monitoring timeout

The update is aborted and no change of master takes place if one of the monitored times exceeds the configured maximum. The fault-tolerant system remains in single mode with the previous master CPU and, assuming certain conditions are met, attempts the master changeover later. For further information, refer to section Time monitoring (Page 114).

Where the values for the monitoring times in the CPUs differ, the higher values always apply.

Calling OB 83

After transferring the parameter data records to the desired modules, OB 83 is called. The sequence is as follows:

1. After you have made the parameter changes to an module in STEP 7 and loaded them in RUN in the CPU, the OB 83 is started (trigger event W#16#3367). Relevant in the OB start information are the logical base address (OB83_MDL_ADDR) and the module type (OB83_MDL_TYPE). From now on, the input and/or initial data of the module might no longer be correct, and no SFCs that send data records to this module may be active.

2. After termination of OB 83, the parameters of the module are reset.

3. After termination of the parameter reset operation, the OB 83 is started again (trigger event W#16#3267 if the parameterization was successful, or W#16#3968 if it was unsuccessful). The input and initial data of the module is the same as after an insertion interrupt, meaning that under certain circumstances may not yet be correct. With immediate effect, you can again call SFCs that send data records to the module.

14.9.6 Step E: Transition to redundant state

Starting situation

The fault-tolerant system operates with the modified parameters in single mode.

Procedure

1. In SIMATIC Manager, select a CPU of the fault-tolerant system, then choose "PLC > Operating Mode" from the menu.
2. From the "Operating Mode" dialog box, select the standby CPU, then click "Warm Restart".

Result

The standby CPU links up and is updated. The fault-tolerant system is operating in redundant mode.

Reaction of the I/O

Type of I/O	One-sided I/O of standby CPU	One-sided I/O of master CPU	Switched I/O
I/O modules	are given new parameter settings[1)] and updated by the CPU.	continue operation without interruption.	
1) Central modules are first reset. Output modules briefly output 0 during this time (instead of the configured substitute or hold values).			

Reaction to monitoring timeout

If one of the monitored times exceeds the configured maximum the update is aborted. The fault-tolerant system remains in single mode with the previous master CPU and, assuming certain conditions are met, attempts to the link-up and update later. For further information, refer to section Time monitoring (Page 114).

Where the values for the monitoring times in the CPUs differ, the higher values always apply.

15 Synchronization modules

15.1 Synchronization modules for S7–400H

Function of the synchronization modules

Synchronization modules are used for communication between two redundant S7-400H CPUs. You require two synchronization modules per CPU, connected in pairs by fiber-optic cable.

The system supports hot-swapping of synchronization modules, and so allows you to influence the repair reaction of the fault-tolerant system and to control the failure of the redundant connection without stopping the plant.

If you remove a synchronization module in redundant mode, there is a loss of synchronization. The standby CPU changes to the TROUBLESHOOTING mode. The other CPU remains master and continues operation in single mode. Once you have inserted the new synchronization module and re-established the redundancy link, the standby CPU links up and updates.

Distance between the S7–400H CPUs

Two types of synchronization module are available:

Order number	Maximum distance between the CPUs
6ES7960–1AA04–0XA0	10 m
6ES7960–1AB04–0XA0	10 km

Long synchronization cables may increase cycle times by up to 10% per cable kilometer.

Note

A fault-tolerant system requires four synchronization modules of the same type.

Mechanical configuration

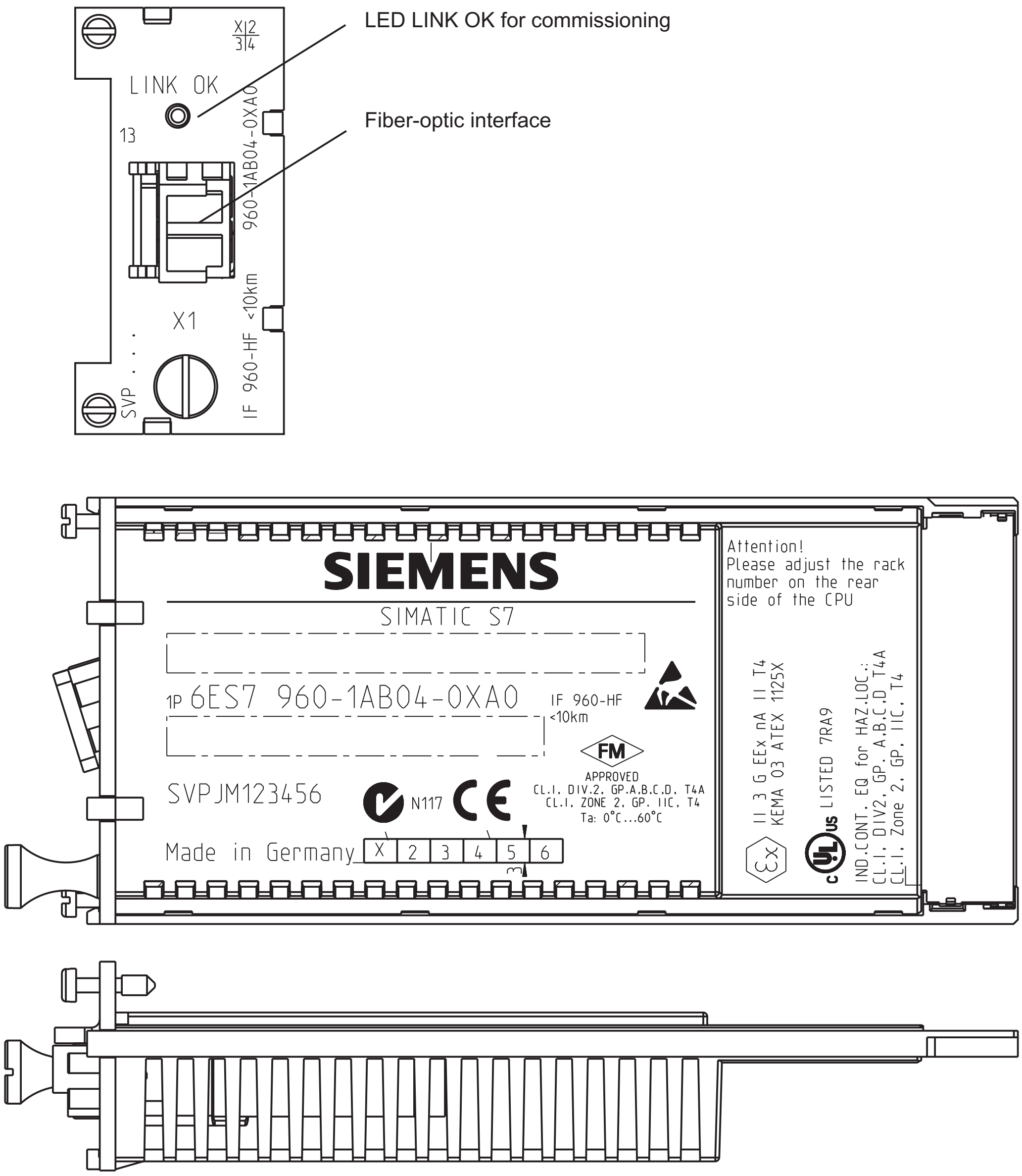


Figure 15-1 Synchronization module

> **⚠ CAUTION**
>
> Risk of injury.
>
> The synchronization module is equipped with a laser system and is classified as a "CLASS 1 LASER PRODUCT" to IEC 60825-1.
>
> Avoid direct contact with the laser beam. Do not open the housing. Always observe the information provided in this manual, and keep the manual to hand as a reference.

CLASS 1 LASER PRODUCT
LASER KLASSE 1 PRODUKT
TO EN 60825

LED LINK OK

During commissioning of the fault-tolerant system, you can use the "LINK OK" LED on the synchronization module to check the quality of the connection between the CPUs.

LED LINK OK	Meaning
Lit	The connection is OK
Flashing	The connection is not reliable, and the signal is disrupted Check the connectors and cables Check whether the fiber-optic cables are installed according to the guidelines in section Installation of fiber-optic cables (Page 283)
Unlit	The connection is interrupted, or there is insufficient light intensity Check the connectors and cables Check whether the fiber-optic cables are installed according to the guidelines in section Installation of fiber-optic cables (Page 283)

OB 84

When operating in redundant mode, the CPU operating system calls OB 84 if it detects a reduced performance in the redundant link between the two CPUs.

Fiber-optic interfaces of unused modules

Fiber-optic interfaces of unused modules must be sealed by dummy plugs during storage to protect the optical equipment. The plugs are in the synchronization module when shipped.

Technical specifications

Technical specifications	6ES7960–1AA04–0XA0	6ES7960–1AB04–0XA0
Maximum distance between the CPUs	10 m	10 km
Supply voltage	5.1 V, supplied by the CPU	5.1 V, supplied by the CPU
Current consumption	210 mA	250 mA
Power loss Wavelength of the optical transceiver	1.1 W 850 nm	1.3 W 1300 nm
Maximal permitted attenuation of the fiber-optic cable	7 dB	12 dB
Maximum permitted difference in cable lengths	9 m	50 m
Dimensions W x H x D (mm)	25 x 53 x 140	25 x 53 x 140
Weight	0.065 kg	0.065 kg

15.2 Installation of fiber-optic cables

Introduction

Fiber-optic cables may only be installed by trained and qualified personnel. Always observe the applicable rules and legislation relating to the safety of buildings. The installation must be carried out with meticulous care, because faulty installations represent the most common source of error. Causes are:

- Kinking of the fiber-optic cable due to an insufficient bending radius.
- Crushing of the cable as a result of excess forces caused by persons treading on the cable, or by pinching, or by the load of other heavy cables.
- Overstretching due to high tensile forces.
- Damage on sharp edges etc.

Permitted bending radius for prefabricated cables

You may not go below the following bending radius when laying the cable:

- Next to connector: 55 mm
- During installation: 60 mm (repeated)
- After installation: 40 mm (one-time)

Points to observe when installing the fiber-optic cables for the S7-400H synchronization link

Always route the two fiber-optic cables separately. This increases availability, and protects the fiber-optic cables from potential double errors caused by simultaneous interruption.

Always make sure the fiber-optic cables are connected to both CPUs before switching on the power supply or the system, otherwise the CPUs may process the user program as the master CPU.

Local quality assurance

Check the points outlined below before you install the fiber-optic cables:

- Does the delivered package contain the correct fiber-optic cables?
- Any visible transport damage to the product?
- Have you organized a suitable intermediate on-site storage for the fiber-optic cables?
- Does the category of the cables match the connecting components?

Storage of the fiber-optic cables

If you do not install the fiber-optic cable immediately after you received the package, it is advisable to store it in a dry location where it is protected from mechanical and thermal influences. Observe the permitted storage temperatures specified in the data sheet of the fiber-optic cable. You should not remove the fiber-optic cables from the original packaging until you are going to install them.

Open installation, wall breakthroughs, cable ducts:

Note the points outlined below when you install fiber-optic cables:

- The fiber-optic cables may be installed in open locations, provided you can safely exclude any damage in those areas (vertical risers, connecting shafts, telecommunications switchboard rooms, etc.).
- Fiber-optic cables should be mounted on mounting rails (cable trays, wire mesh ducts) using cable ties. Take care not to crush the cable when you fasten it (see Pressure).
- Always deburr or round the edges of the breakthrough before you install the fiber-optic cable, in order to prevent damage to the sheathing when you pull in and fasten the cable.
- The bending radii must not be smaller than the value specified in the manufacturer's data sheet.
- The branching radii of the cable ducts must correspond to the specified bending radius of the fiber-optic cable.

Cable pull-in

Note the points below when pulling-in fiber-optic cables:

- Always observe the information on pull forces in the data sheet of the corresponding fiber-optic cable.
- Do not reel off any greater lengths when you pull in the cables.
- Install the fiber-optic cable directly from the cable drum wherever possible.
- Do not spool the fiber-optic cable sideways off the drum flange (risk of twisting).
- You should use a cable pulling sleeve to pull in the fiber-optic cable.
- Always observe the specified bending radii.
- Do not use any grease- or oil-based lubricants.
  You may use the lubricants listed below to support the pulling-in of fiber-optic cables.
  - Yellow compound (Wire-Pulling, lubricant from Klein Tools; 51000)
  - Soft soap
  - Dishwashing liquid
  - Talcum powder
  - Detergent

Pressure

Do not exert any pressure on the cable, for example, by the improper use of clamps (cable quick-mount) or cable ties. Your installation should also prevent anyone from stepping onto the cable.

Influence of heat

Fiber-optic cables are highly sensitive to direct heat, so the cables must not be worked on using hot-air guns or gas burners as used in heat-shrink tubing technology.

15.3 Selecting fiber-optic cables

Make allowance for the following conditions and situations when selecting a suitable fiber-optic cable:

- Required cable lengths
- Indoor or outdoor installation
- Any particular protection against mechanical stress required?
- Any particular protection against rodents required?
- Installation of an outdoor cable directly underground?
- Does the fiber-optic cable have to be water-proof?
- Which temperatures influence the installed fiber-optic cable?

Cable lengths up to 10 m

The synchronization module 6ES7960–1AA04–0XA0 can be operated in pairs with fiber-optic cables up to a length of 10 m.

Select cables with the following specification for lengths up to 10 m:

- Multimode fiber 50/125 µ or 62,5/125 µ
- Patch cable for indoor applications
- 2 x duplex cable per fault-tolerant system, crossed
- Connector type LC–LC

The following lengths of such cables are available as accessories for fault-tolerant systems

Table 15-1 Accessory fiber-optic cable

Length	Order number
1 meter	6ES7960–1AA04–5AA0
2 m	6ES7960–1AA04–5BA0
10 m	6ES7960–1AA04–5KA0

Cable length up to 10 km

The synchronization module 6ES7960–1AA04–0XA0 can be operated in pairs with fiber-optic cables up to a length of 10 km.

The following rules apply:

- Make sure there is enough strain relief on the modules if you use fiber optic cables longer than 10 m.
- Keep to the specified ambient operating conditions of the fiber-optic cables used (bending radii, pressure, temperature...)
- Observe the technical specifications of the fiber optic cable (attenuation, bandwidth...)

Fiber-optic cables with lengths above 10 m usually have to be custom-made. In the first step, select the following specification:

- Single-mode fiber (mono-mode fiber) 9/125 µ

  For short lengths required for testing and commissioning you may also use the lengths up to 10 m available as accessories. For continuous use, only the specified cables with monomode fibers are permitted.

The table below shows the further specifications, based on your application:

Table 15-2 Specification of fiber-optic cables for indoor applications

Cabling	Components required	Specification
The entire cabling is routed within a building No cable junction is required between the indoor and outdoor area The necessary cable length is available in one piece. There is no need to connect several cable segments by means of distribution boxes. Complete installation using prefabricated patch cables	Patch cables	2 x duplex cable per system Connector type LC-LC Crossed cores Further specifications you may need to observe for your plant: UL certification Halogen-free materials
	Prefabricated cable	Multicore cables, 4 cores per system Connector type LC-LC Crossed cores Further specifications you may need to observe for your plant: UL certification Halogen-free materials

Cabling	Components required	Specification
The entire cabling is routed within a building No cable junction is required between the indoor and outdoor area The necessary cable length is available in one piece. There is no need to connect several cable segments by means of distribution boxes. Complete installation using prefabricated patch cables	including patch cables for indoor applications as required	1 cable with 4 cores per fault-tolerant system Both interfaces in one cable 1 or 2 cables with several shared cores Separate installation of the interfaces in order to increase availability (reduction of common cause factor) Connector type ST or SC, for example, to match other components; see below Further specifications you may need to observe for your plant: UL certification Halogen-free materials Avoid spliced cables in the field. Use prefabricated cables with pulling protection/aids in whiplash or breakout design, including measuring log.
	Patch cable for indoor applications	Connector type LC on ST or SC, for example, to match other components
Installation using distribution boxes, see Fig. 13 -2	One distribution/junction box per branch Installation cables and patch cables are interconnected by means of distribution box, using either ST or SC connectors for example. Check the cross-over installation when you wire the CPUs.	Connector type ST or SC, for example, to match other components

Table 15-3 Specification of fiber-optic cables for outdoor applications

Cabling	Components required	Specification
A cable junction is required between the indoor and outdoor area see Figure 13-2	• Installation cables for outdoor applications	Installation cables for outdoor applications • 1 cable with 4 cores per fault-tolerant system Both interfaces in one cable • 1 or 2 cables with several shared cores Separate installation of the interfaces in order to increase availability (reduction of common cause factor) • Connector type ST or SC, for example, to match other components; see below Further specifications you may need to observe for your plant: • UL certification • Halogen-free materials Observe further specifications as required for local conditions: • Protection against increased mechanical stress • Protection against rodents • Water-proofing • Suitable for direct underground installation • Suitable for the given temperature ranges Avoid spliced cables in the field. Use prefabricated cables with pulling protection/aids in whiplash design, including measuring log.
	• including installation cables for indoor applications as required	• 1 cable with 4 cores per fault-tolerant system Both interfaces in one cable • 1 or 2 cables with several shared cores Separate installation of the interfaces in order to increase availability (reduction of common cause factor) • Connector type ST or SC, for example, to match other components; see below Further specifications you may need to observe for your plant: • UL certification • Halogen-free materials Avoid spliced cables in the field. Use prefabricated cables with pulling protection/aids in whiplash or breakout design, including measuring log.
	• Patch cable for indoor applications	• Connector type LC on ST or SC, for example, to match other components

Cabling	Components required	Specification
A cable junction is required between the indoor and outdoor area see Figure 13-2	• One distribution/junction box per branch Installation cables and patch cables are interconnected by means of distribution box, using either ST or SC connectors for example. Check the cross-over installation when you wire the CPUs.	• Connector type ST or SC, for example, to match other components

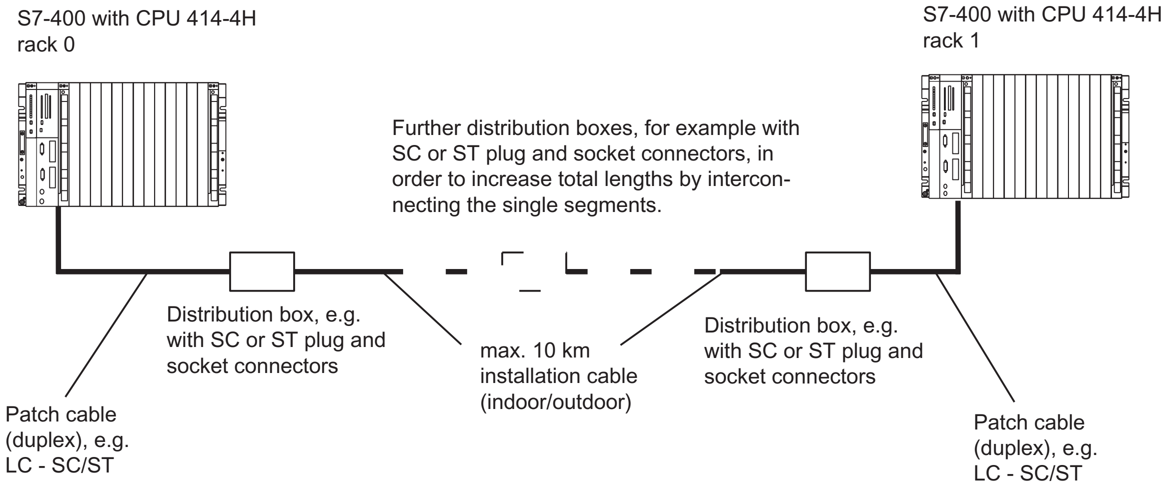


Figure 15-2 Fiber-optic cables, installation using distribution boxes

16 S7-400 cycle and reaction times

This section describes the decisive factors in the cycle and reaction times of your of S7-400 station.

You can read out the cycle time of the user program from the relevant CPU using the programming device (refer to the manual *Configuring Hardware and Connections with STEP 7*).

The examples included show you how to calculate the cycle time.

An important aspect of a process is its reaction time. How to calculate this factor is described in detail in this section. When operating a CPU 41x-H as master on the PROFIBUS-DP network, you also need to include the additional DP cycle times in your calculation (see section Reaction time (Page 304)).

Further information

For more detailed information on the following execution times, refer to the Instruction list S7–400H. This lists all the *STEP 7* instructions that can be executed by the particular CPUs along with their execution times and all the SFCs/SFBs integrated in the CPUs and the IEC functions that can be called in *STEP 7* with their execution times.

16.1 Cycle time

This section describes the decisive factors in the cycle time, and how to calculate it.

Definition of cycle time

The cycle time is the time the operating system requires to execute a program, i.e. to execute OB 1, including all interrupt times required by program elements and for system activities.

This time is monitored.

Time slice model

The program, and so also the user program, is executed cyclically in time slices. To demonstrate the processes, let us presume a global time slice length of exactly 1 ms.

Process image

The CPU reads and writes the process signals to a process image before it starts cyclic program execution, in order to obtain a precise image of the process signals. The CPU does not access the signal modules directly when the I/O operand areas respond during program execution, but rather addresses its memory area which contains the I/O process image.

Phases in cyclic program execution

The table below shows the various phases in cyclic program execution.

Table 16-1 Cyclic program execution

Step	Sequence
1	The operating system initiates the cycle monitoring time.
2	The CPU writes the values of the process image to the outputs of the output modules.
3	The CPU reads the status of inputs of the input modules, and then updates the process image of the inputs.
4	The CPU executes the user program in time slices, and executes the operations defined in the program.
5	At the end of the cycle, the operating system performs all pending tasks, such as loading or deleting blocks.
6	Finally, on expiration of any given minimum cycle time, the CPU returns to the start of the cycle and restarts cycle monitoring.

Elements of the cycle time

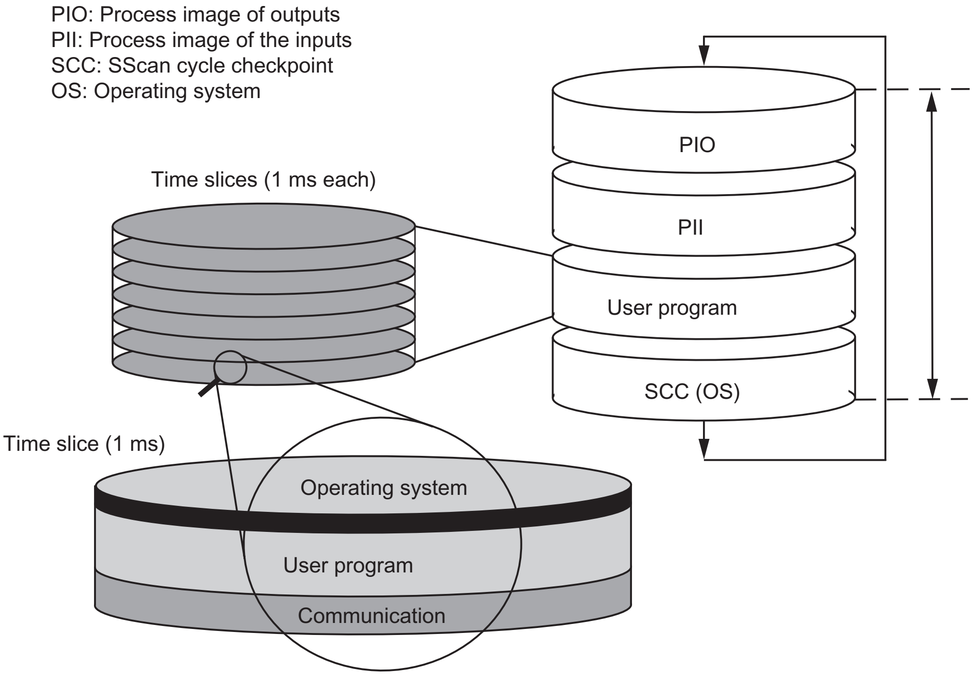


Figure 16-1 Elements and composition of the cycle time

16.2 Calculating the cycle time

Extension of the cycle time

The cycle time of a user program is extended by the factors outlined below:

- Time-based interrupt execution
- Hardware interrupt handling (see also section Interrupt reaction time (Page 314))
- Diagnostics and error processing (see also section Example of calculation of the interrupt reaction time (Page 316))
- Communication via MPI and CPs connected to the communication bus (e.g.: Ethernet, Profibus, DP) as a factor in communication load
- Special functions such as controlling and monitoring tags or the block status
- Download and deletion of blocks, compression of user program memory

Influencing factors

The table below shows the factors influencing the cycle time.

Table 16-2 Factors influencing cycle time

Factors	Comment
Transfer time for the process image of outputs (PIO) and inputs (PII)	See tables from 16-3 onwards
User program execution time	This value is calculated based on the execution times of the various statements (see the *S7-400 statement list*).
Operating system execution time at the scan cycle checkpoint	See table 16-7
Extension of cycle time due to communication load	You configure the maximum permitted communication load on the cycle as a percentage in **STEP 7** (*Programming with STEP 7* manual). See section Communication load (Page 301).
Load on cycle times due to interrupts	Interrupt requests can always stop user program execution. See Table 16-8

Process image update

The table below shows the time a CPU requires to update the process image (process image transfer time). The specified times only represent "ideal values", and may be extended accordingly by any interrupts or communication of the CPU.

Calculation of the transfer time for process image update:

C+ portion in the central unit (taken from row A of the table below)
+ portion in the expansion unit with local link (from row B)
+ portion in the expansion unit with remote link (from row C)
+ portion via the integrated DP interface (from row D)
+ portion of consistent data via the integrated DP interface (from row E1)
+ portion of consistent data via external DP interface (from row E2)

= Transfer time for process image update

The tables below show the various portions of the transfer time for a process image update (process image transfer time). The specified times only represent "ideal values", and may be extended accordingly by any interrupts or communication of the CPU.

Table 16-3 Allocation of the process image transfer time, CPU 412-3H

	Allocation **n = number in bytes in the process image** **m = number of accesses to process image*)**	**CPU 412-3H stand-alone mode**	**CPU 412-3H redundant**
K	Base load	13 µs	16 µs
A **)	In central unit Read/write byte/word/double word	m * 9.5 µs	m * 40 µs
B **)	In expansion unit with local link Read/write byte/word/double word	m * 24 µs	m * 52 µs
C **)***)	In expansion unit with remote link Read/write byte/word/double word	m * 48 µs	m * 76 µs
D	In the DP area for the integrated DP interface Read byte/word/double word	m * 2.0 µs	m * 35 µs
D	In the DP area for the external DP interfaces Read/write byte/word/double word	m * 6.0 µs	m * 40 µs
E1	Consistent data in the process image for the integrated DP interface Read/write data	n * 1.4 µs	n * 4.4 µs
E2	Consistent data in the process image for the external DP interface (CP 443–5 extended) read/write data	n * 3.0 µs	n * 6.5 µs
*) The module data is updated with the minimum number of accesses. (e.g.: 8 bytes result in 2 double word accesses, and 16 bytes in 4 double word accesses.)			
**) In the case of I/O inserted into the central unit or into an expansion unit, the specified value contains the execution time of the I/O module			
***)Measured with IM460-3 and IM461-3, at a link length of 100 m			

Table 16-4 Portion of the process image transfer time, CPU 414–4H

	Allocation n = number in bytes in the process image m = number of accesses to process image*)	CPU 414–4H stand-alone mode	CPU 414–4H redundant mode
K	Base load	8 μs	9 μs
A **)	In central unit Read/write byte/word/double word	m * 8.5 μs	m * 25.7 μs
B **)	In expansion unit with local link Read/write byte/word/double word	m * 23 μs	m * 40 μs
C **)***)	In expansion unit with remote link Read/write byte/word/double word	m * 58 μs	m * 64 μs
D	In the DP area for the integrated DP interface Read byte/word/double word	m * 1.3 μs	m * 21.5 μs
D	In the DP area for the external DP interfaces Read/write byte/word/double word	m * 5.2 μs	m * 24.6 μs
E1	Consistent data in the process image for the integrated DP interface Read/write data	n * 0.66 μs	n * 3.1 μs
E2	Consistent data in the process image for the external DP interface (CP 443–5 extended) read/write data	n * 2.5 μs	n * 6.5 μs
*) The module data is updated with the minimum number of accesses. (e.g.: 8 bytes result in 2 double word accesses, and 16 bytes in 4 double word accesses.)			
**) In the case of I/O inserted into the central unit or into an expansion unit, the specified value contains the execution time of the I/O module			
***)Measured with IM460-3 and IM461-3 at a link length of 100 m			

Table 16-5 Portion of the process image transfer time, CPU 417-4H

	Allocation n = number in bytes in the process image m = number of accesses to process image*)	CPU 417–4H stand-alone mode	CPU 417–4H redundant mode
K	Base load	3 µs	4 µs
A **)	In central unit Read/write byte/word/double word	m * 7.3 µs	m * 15.7 µs
B **)	In expansion unit with local link Read/write byte/word/double word	m * 20 µs	m * 26 µs
C **)***)	In expansion unit with remote link Read/write byte/word/double word	m * 45 µs	m * 50 µs
D	In the DP area for the integrated DP interface Read byte/word/double word	m * 1.2 µs	m * 13 µs
D	In the DP area for the external DP interface Read/write byte/word/double word	m * 5 µs	m * 15 µs
E1	Consistent data in the process image for the integrated DP interface Read/write data	n * 0.25 µs	n * 2.5 µs
E2	Consistent data in the process image for the external DP interface (CP 443–5 extended) read/write data	n * 2.25 µs	n * 3.4 µs
*) The module data is updated with the minimum number of accesses. (e.g.: 8 bytes result in 2 double word accesses, and 16 bytes in 4 double word accesses.)			
**) In the case of I/O inserted into the central unit or into an expansion unit, the specified value contains the execution time of the I/O module			
***)Measured with IM460-3 and IM461-3 at a link length of 100 m			

Extension of the cycle time

The calculated cycle time of a S7-400H CPU must be multiplied by a CPU-specific factor. The table below lists these factors:

Table 16-6 Extension of the cycle time

Startup	412-3H stand-alone mode	412-3H redundant	414-4H stand-alone mode	414-4H redundant mode	417-4H stand-alone mode	417-4H redundant mode
Factor	1,04	1,2	1,05	1,2	1,05	1,2

Long synchronization cables may further increase cycle times. By up to 10% per cable kilometer.

Operating system execution time at the scan cycle checkpoint

The table below shows the operating system execution time at the cycle checkpoint of the CPUs.

Table 16-7 Operating system execution time at the scan cycle checkpoint

Sequence	412-3H stand-alone mode	412-3H redundant	414-4H stand-alone mode	414-4H redundant	417-4H stand-alone mode	417-4H redundant
Cycle control at the SCCP	271-784 µs ∅ 284 µs	679-1890 µs ∅ 790 µs	198-553 µs ∅ 204 µs	548-1417 µs ∅ 609 µs	83 - 315 µs ∅ 85 µs	253 - 679 µs ∅ 270 µs

Cycle time extension due to nested interrupts

Table 16-8 Cycle time extension due to nested interrupts

CPU	Process interrupt	Diagnostic interrupt	Time-of-day interrupt	Delay interrupt	Watchdog interrupt	Programming / I/O access error	Asynchronous error
CPU 412-3 H stand-alone mode	481 µs	488 µs	526 µs	312 µs	333 µs	142 µs / 134 µs	301 µs
CPU 412-3 H redundant mode	997 µs	843 µs	834 µs	680 µs	674 µs	427 µs / 179 µs	832 µs
CPU 414–4 stand-alone mode	315 µs	326 µs	329 µs	193 µs	189 µs	89 µs / 85 µs	176 µs
CPU 414–4 H redundant mode	637 µs	539 µs	588 µs	433 µs	428 µs	272 µs / 114 µs	252 µs
CPU 417-4 stand-alone mode	160 µs	184 µs	101 µs	82 µs	120 µs	36 µs / 35 µs	90 µs
CPU 417-4 H redundant mode	348 µs	317 µs	278 µs	270 µs	218 µs	121 µs / 49 µs	115 µs

Add the program execution time at interrupt level to this extension value.

The corresponding times are added together if the program contains nested interrupts.

16.3 Different cycle times

The cycle time (T_{cyc}) is not of the same length for every cycle. The figure below shows the different cycle times T_{cyc1} and T_{cyc2}. T_{cyc2} is longer than T_{cyc1} because the cyclically executed OB 1 is interrupted by a TOD interrupt OB (here: OB 10).

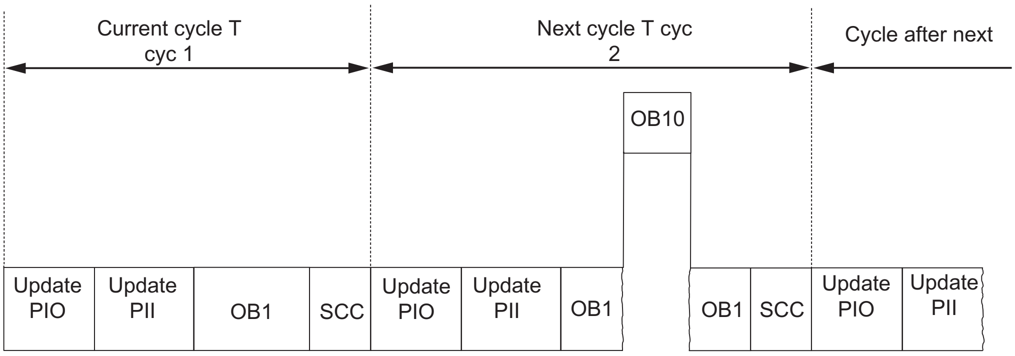


Figure 16-2 Different cycle times

A further factor in different cycle times is the variable block execution time (e.g. OB 1) caused by:

- conditional statements,
- conditional block calls,
- different program paths,
- loops etc.

Maximum cycle time

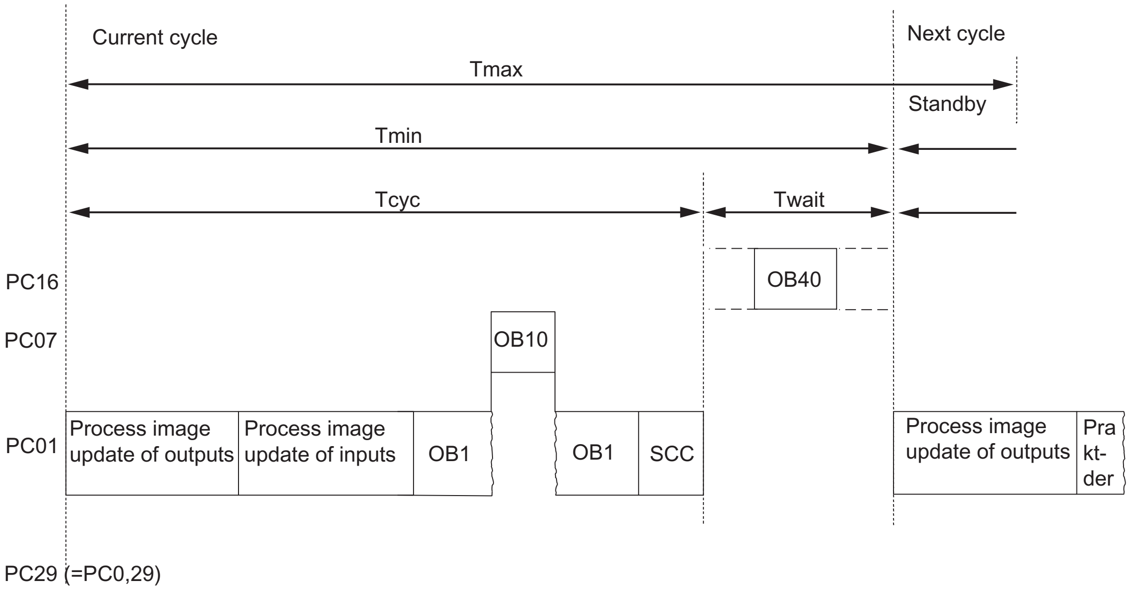
You can edit the default maximum cycle time (cycle monitoring time) in STEP 7. On expiration of this time OB 80 is called, in which you can define the CPU's reaction to the timeout error. Provided you do not retrigger the cycle time using SFC 43, OB 80 doubles the cycle time on its first call. In this case the CPU goes into STOP on the second call of OB 80.

The CPU goes into STOP if there is no OB 80 in its memory.

Minimum cycle time

You can set the minimum CPU cycle time in STEP 7. This is useful if you

- want to set an interval of approximately the same length between the program execution cycles of OB1 (free cycle), or
- prevent unnecessary process image updates if the cycle time is too short



Tmin = configurable minimum cycle time
Tmax = configurable maximum cycle time
Tcyc = the cycle time
Twait = difference between Tmin and the actual cycle time. Within this time you can process interrupt events or SCC tasks
PC = Priority Class

Figure 16-3 Minimum cycle time

The actual cycle time is derived from the sum of T_{cyc} and T_{wait}. So it is always greater than or equal to T_{min}.

16.4 Communication load

The operating system provides the CPU continuously with the configured time slices as a percentage of the overall CPU processing resources (time slice technique). If this processing capacity is not required for communication, it is made available to the other processes.

You can set a communication load between 5 % and 50 % in your hardware configuration. The default value is 20 %.

This percentage is to be interpreted as mean value, i.e. communication resources may take significantly more than 20 % of a time slice. The communication then only takes a few or 0 % in the next time slice.

The formula below describes the influence of communication load on the cycle time:

$$\text{Actual cycle time} = \text{Cycle time} \times \frac{100}{100 - \text{"Configured communication load in \%"}}$$

Round the result up to the next highest integer !

Figure 16-4 Formula: Influence of communication load

Data consistency

The user program is interrupted to process communications. This interruption can be triggered after any statement. These communication requests may lead to a change in user data. As a result, data consistency cannot be ensured over several accesses.
How to ensure data consistency in operations comprising more than one command is described in the "Consistent data" section.

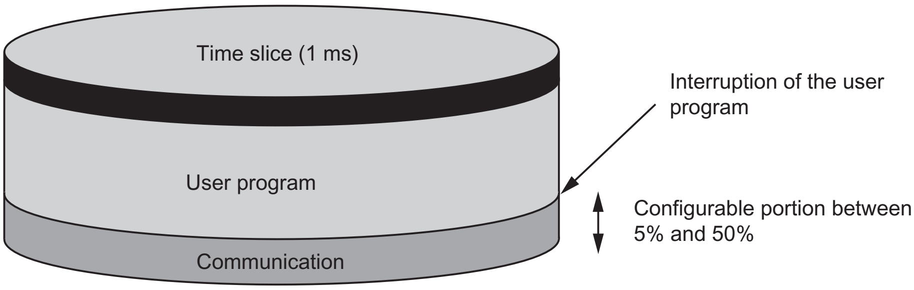


Figure 16-5 Distribution of a time slice

The operating system takes a certain portion of the remaining time slice for internal tasks. This portion is included in the factor defined in the tables starting at 16-3.

Example: 20 % communication load

In the hardware configuration, you have set a communication load of 20 %.

The calculated cycle time is 10 ms.

This means that a setting of 20 % communication load allocates an average of 200 μs to communication and 800 μs to the user program in each time slice. So the CPU requires 10 ms / 800 μs = 13 time slices to execute one cycle. This means the physical cycle time is equivalent to 13 times 1-ms time slice = 13 ms, if the CPU fully utilizes the configured communication load.

That is to say, 20 % communication does not extend the cycle by a linear amount of 2 ms, but by 3 ms.

Example: 50 % communication load

In the hardware configuration, you have set a communication load of 50 %.

The calculated cycle time is 10 ms.

This means that 500 μs remain in each time slice for the cycle. So the CPU requires 10 ms / 500 μs = 20 time slices to execute one cycle. This means the physical cycle time is 20 ms if the CPU fully utilizes the configured communication load.

So a setting of 50 % communication load allocates 500 μs to communication and 500 μs to the user program in each time slice. So the CPU requires 10 ms / 500 μs = 20 time slices to execute one cycle. This means the physical cycle time is equivalent to 20 times 1-ms time slice = 20 ms, if the CPU fully utilizes the configured communication load.

This means that 50 % communication does not extend the cycle by a linear amount of 5 ms, but by 10 ms (= doubling the calculated cycle time).

Dependency of the actual cycle time on communication load

The figure below describes the non-linear dependency of the actual cycle time on communication load. In our example, we have chosen a cycle time of 10 ms.

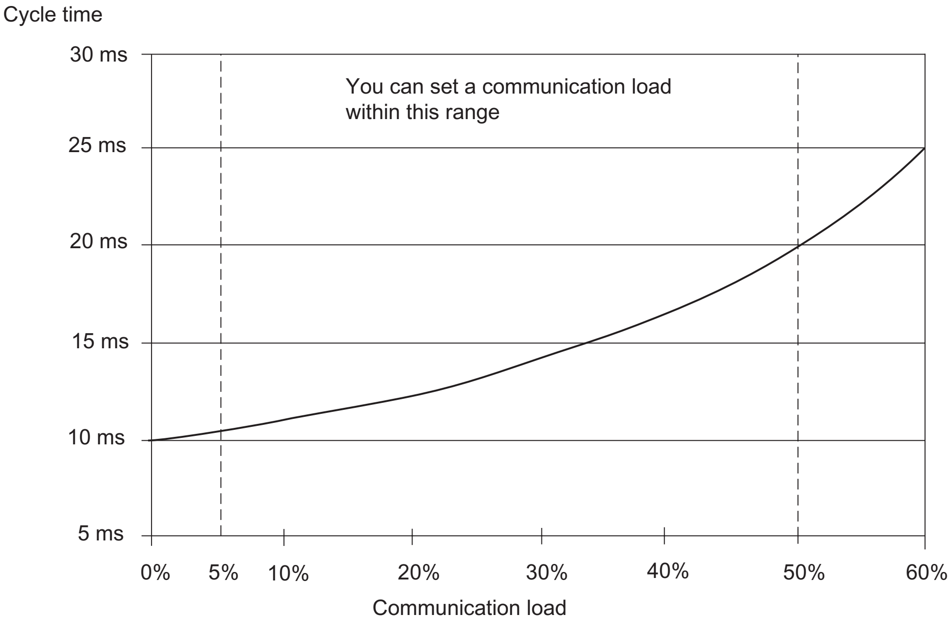


Figure 16-6 Dependency of the cycle time on the communication load

Further effects on the actual cycle time

Seen statistically, the extension of cycle times due to communication load leads to more asynchronous events occurring within an OB1 cycle, for example interrupts. This further extends the OB1 cycle. How much it is extended depends on the number of events per OB1 cycle and the time required for processing these events.

Remarks

- Change the value of the "communication load" parameter to check the effects on the cycle time during system runtime.
- Always take the communication load into account when you set the maximum cycle time, otherwise you risk timeouts.

Recommendations

- Use the default setting wherever possible.
- Increase this value only if the CPU is used primarily for communication, and if time is not a critical factor for the user program! In all other situations you should only reduce this value!

16.5 Reaction time

Definition of reaction time

The reaction time represents the time expiring between the detection of an input signal and the modification of its logically linked output signal.

Fluctuation length

The actual reaction time lies between the shortest and longest reaction time. Always expect the longest reaction time when you configure your system.

The section below deals with the shortest and longest reaction times, in order to provide an overview of the fluctuation in the length of reaction times.

Factors

The reaction time is determined by the cycle time and the following factors:

- Delay at the inputs and outputs
- Additional DP cycle times on the PROFIBUS DP network
- Processing in the user program

Delay of the I/Os

Make allowances for the following module-specific delay times:

- For digital inputs: the input delay time
- For digital inputs with interrupt function: the input delay time + internal preparation time
- For digital outputs: negligible delay times
- For relay outputs: typical delay times of 10 ms to 20 ms.
  The delay of relay outputs also depends on the temperature and voltage.
- For analog inputs: cycle time for analog input
- For analog outputs: response time at analog outputs

For information on delay times, refer to the technical specifications of the signal modules.

DP cycle times on the PROFIBUS DP network

If you configured your PROFIBUS DP network in **STEP 7**, **STEP 7** calculates the typical DP cycle time to be expected. You can then view the DP cycle time of your configuration on the PG in the bus parameters section.

The figure below provides an overview of the DP cycle times. In this example, we assume an average value for each DP slave of 4 bytes of data.

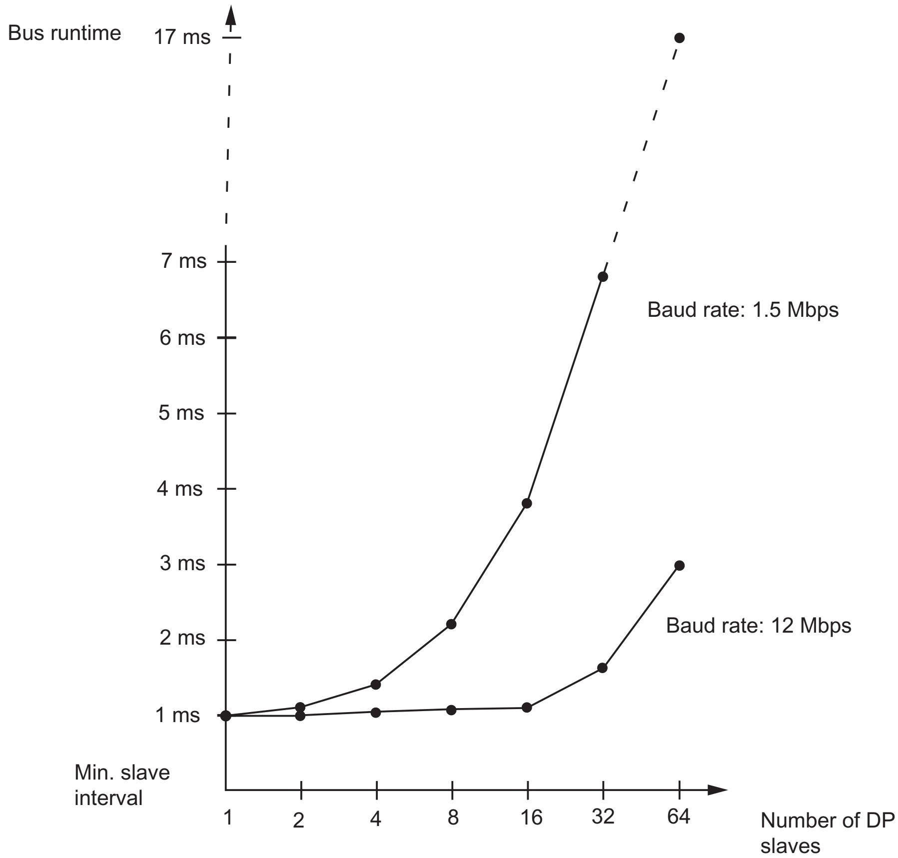


Figure 16-7 DP cycle times on the PROFIBUS DP network

If you are operating a PROFIBUS-DP network with more than one master, you will need to take the DP cycle time into account for each master. In other words, perform a separate calculation for each master and add the results together.

Shortest reaction time

The following figure illustrates the conditions under which the shortest reaction time can be achieved.

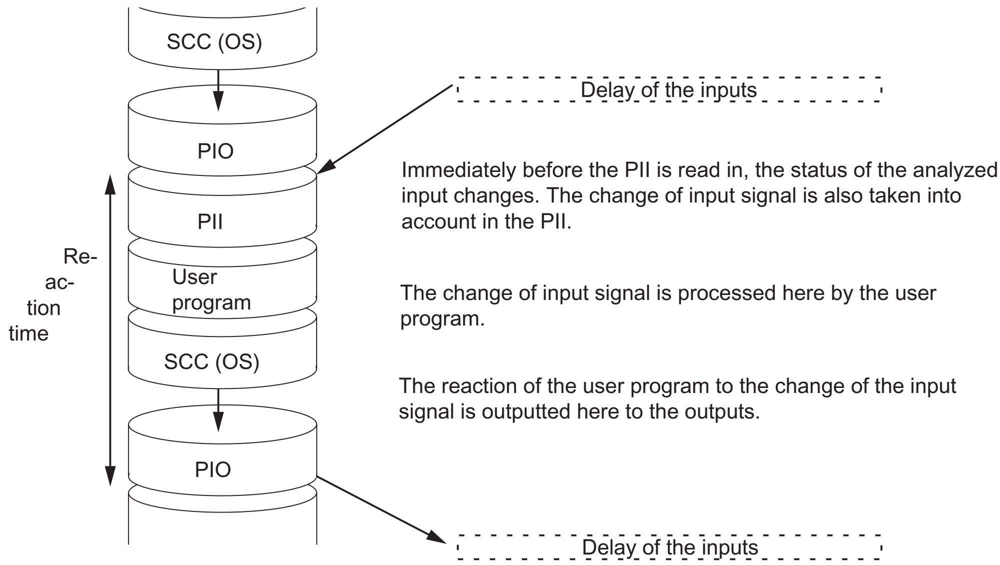


Figure 16-8 Shortest reaction time

Calculation

The (shortest) reaction time is made up as follows:

- 1 × process image transfer time of the inputs +
- 1 × process image transfer time of the outputs +
- 1 x program processing time, +
- 1 x operating system processing time at the SCCP +
- Delay at the inputs and outputs

The result is equivalent to the sum of the cycle time plus the I/O delay times.

Note

If the CPU and signal module are not in the central unit, you will have to add twice the delay time of the DP slave frame (including processing in the DP master).

Longest reaction time

The figure below shows the conditions under which the longest reaction time is reached.

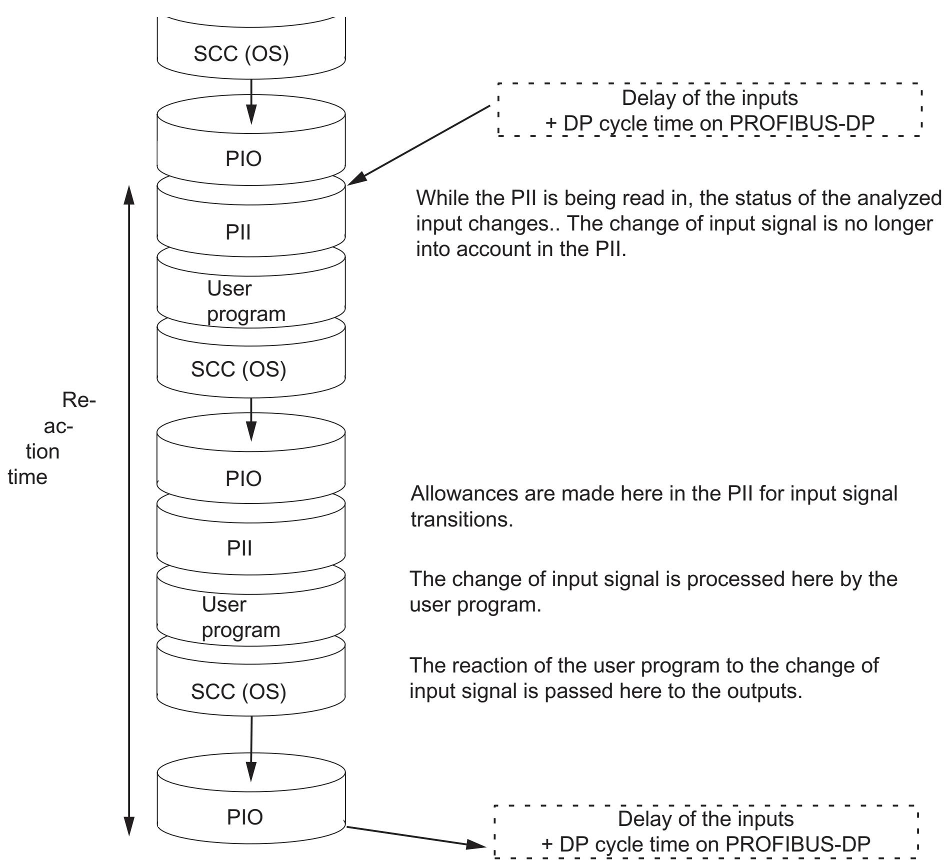


Figure 16-9 Longest reaction time

Calculation

The (longest) reaction time is made up as follows:

- 2 × process image transfer time of the inputs +
- 2 × process image transfer time of the outputs +
- 2 x operating system processing time +
- 2 x program processing time, +
- 2 x delay of the DP slave frame (including processing in the DP master) +
- Delay at the inputs and outputs

This is equivalent to the sum of twice the cycle time and the delay in the inputs and outputs plus twice the DP cycle time.

I/O direct access

You can achieve faster reaction times with direct access to the I/O in your user program, for example with

- L PIB or
- T PQW.

You can work around the reaction times as shown earlier.

Reducing the reaction time

This reduces the maximum reaction time to

- Delay at the inputs and outputs
- User program execution time (can be interrupted by higher-priority interrupt handling)
- Runtime of direct access
- Twice the bus delay time of DP

The following table lists the execution times of direct access by the CPU to I/O modules. The times shown are "ideal values".

Table 16-9 Direct access of the CPUs to I/O modules

Access mode	412-3H stand-alone mode	412-3H redundant	414-4H stand-alone mode	414-4H redundant	417-4H stand-alone mode	417-4H redundant
Read byte	3.5 µs	30.5 µs	3.0 µs	21.0 µs	2.2 µs	11.2 µs
Read word	5.2 µs	33.0 µs	4.5 µs	22.0 µs	3.9 µs	11.7 µs
Read double word	8.2 µs	33.0 µs	7.6 µs	23.5 µs	7.0 µs	14.7 µs
Write byte	3.5 µs	31.1 µs	2.8 µs	21.5 µs	2.3 µs	11.3 µs
Write word	5.2 µs	33.5 µs	4.5 µs	22.5 µs	3.9 µs	11.8 µs
Write double word	8.5 µs	33.5 µs	7.8 µs	24.0 µs	7.1 µs	15.0 µs

Table 16-10 Direct access of the CPUs to I/O modules in the expansion unit with local link

Access mode	412-3H stand-alone mode	412-3H redundant	414-4H stand-alone mode	414-4H redundant	417-4H stand-alone mode	417-4H redundant
Read byte	6.9 µs	32.6 µs	6.3 µs	22.5 µs	5.7 µs	13.4 µs
Read word	12.1 µs	36.5 µs	11.5 µs	27.5 µs	10.8 µs	18.6 µs
Read double word	22.2 µs	46.5 µs	21.5 µs	37.5 µs	20.9 µs	28.7 µs
Write byte	6.6 µs	31.6 µs	5.9 µs	22.5 µs	5.5 µs	13.4 µs
Write word	11.7 µs	36.7 µs	11.0 µs	27.5 µs	10.4 µs	18.3 µs
Write double word	21.5 µs	46.4 µs	20.8 µs	37.0 µs	20.2 µs	28.0 µs

Table 16-11 Direct access of the CPUs to I/O modules in the expansion unit with remote link

Access mode	412-3H stand-alone mode	412-3H redundant	414-4H stand-alone mode	414-4H redundant	417-4H stand-alone mode	417-4H redundant
Read byte	11.5 µs	35.0 µs	11.5 µs	26.0 µs	11.3 µs	17.0 µs
Read word	23.0 µs	47.0 µs	23.0 µs	37.5 µs	22.8 µs	28.6 µs
Read double word	46.0 µs	70.0 µs	46.0 µs	60.5 µs	45.9 µs	51.7 µs
Write byte	11.0 µs	35.0 µs	11.0 µs	26.0 µs	10.8 µs	16.8 µs
Write word	22.0 µs	46.0 µs	22.0 µs	37.0 µs	21.9 µs	27.8 µs
Write double word	44.5 µs	68.5 µs	44.5 µs	59.0 µs	44.0 µs	50.0 ms

The specified times are purely CPU processing times and apply, unless otherwise stated, to signal modules in the central unit.

Note

You can also achieve fast reaction times by using hardware interrupts; see section Interrupt reaction time (Page 314).

16.6 Calculating cycle and reaction times

Cycle time

1. Using the Instruction List, determine the runtime of the user program.
2. Calculate and add the transfer time for the process image. You will find guide values for this in the tables starting at 16-3.
3. Add to it the processing time at the cycle checkpoint. You will find guide values for this in Table 16–8.
4. Multiply the calculated value by the factor in Table 16–7.

The result is the **cycle time.**

Extension of the cycle time due to communication and interrupts

1. Multiply the result by the following factor:

100 / (100 – "configured communication load in %")

1. Using the instruction list, calculate the runtime of the program elements processing the interrupts. To do so, add the relevant value from Table 16-9.
   Multiply this value by the factor from step 4.
   Add this value to the theoretical cycle time as often as the interrupt is triggered or is expected to be triggered during the cycle time.

The result you obtain is approximately the **actual cycle time.** Make a note of the result.

Table 16-12 Example of calculating the reaction time

Shortest reaction time	Longest reaction time
7. Next, calculate the delays in the inputs and outputs and, if applicable, the cycle times on the PROFIBUS DP network.	7. Multiply the actual cycle time by the factor 2.
	8. Next, calculate the delays in the inputs and outputs and the cycle times on the PROFIBUS DP network.
8. The result you obtain is the **shortest reaction time**.	9. The result you obtain is the **longest reaction time**.

16.7 Examples of calculating the cycle and reaction times

Example I

You have installed an S7-400 with the following modules in the central unit

- a 414-4H CPU in redundant mode
- 2 digital input modules SM 421; DI 32xDC 24 V (each with 4 bytes in the PI)
- 2 digital output modules SM 422; DO 32xDC 24 V /0.5 (each with 4 bytes in the PI)

User program

According to the operation list, your user program has a runtime of 15 ms.

Calculating the cycle time

The cycle time for the example is derived from the following times:

- As the CPU-specific factor is 1.2, the user program execution time is:
  approx. 18.0 ms
- Process image transfer time (4 x double-word access)

  Process image: 9 μs + 4 ×25.7 μs = approx. 0.112 ms
- OS execution time at the cycle checkpoint:
  approx. 0.609 ms

The cycle time is obtained from the sum of the listed times:

Cycle time = 18.0 ms + 0.112 ms + 0.609 ms **= 18.721 ms.**

Calculating the actual cycle time

- Allowance for communication load (default value: 20%):
  18.721 ms * 100 / (100-20) **= 23.401 ms.**
- There is no interrupt handling.

So the actual cycle time rounded up is **23.5 ms.**

Calculating the longest reaction time

- Longest reaction time
  23.5 ms * 2 **= 47.0 ms.**
- The delay of the inputs and outputs is negligible.
- All the components are plugged into the central rack; DP cycle times do not therefore have to be taken into account.
- There is no interrupt handling.

So the longest reaction time rounded up is **= 47 ms.**

Example II

You have installed an S7-400 with the following modules:

- a 414-4H CPU in redundant mode
- 4 digital input modules SM 421; DI 32xDC 24 V (each with 4 bytes in the PI)
- 3 digital output modules SM 422; DO 16xDC 24 V /2 (each with 2 bytes in the PI)
- 2 analog input modules SM 431; AI 8x13 bit (not in the PI)
- 2 analog output modules SM 432; AO 8x13 bit (not in the PI)

CPU parameters

The CPU has been assigned parameters as follows:

- Cycle load due to communication: 40 %

User program

According to the operation list, your user program has a runtime of 10.0 ms.

Calculating the cycle time

The theoretical cycle time for the example is derived from the following times:

- As the CPU-specific factor is 1.2, the user program execution time is:
  approx. 12.0 ms
- Process image transfer time (4 x double-word access and 3 x word access)

  Process image: 9 µs + 7 ×25.7 µs = approx. 0.189 ms
- OS runtime at the cycle checkpoint:
  approx. 0.609 ms

The cycle time is obtained from the sum of the listed times:

Cycle time = 12.0 ms + 0.189 ms + 0.609 ms **= 12.789 ms.**

Calculating the actual cycle time

- Allowance for communication load:
  12.789 ms * 100 / (100-40) **= 21.33 ms.**
- A time-of-day interrupt with a runtime of 0.5 ms is triggered every 100 ms.
  The interrupt can be triggered a maximum of one time during a cycle:
  0.5 ms + 0.588 ms (from table 16-9) **= 1.088 ms.**
  Allowing for communication load:
  1.088 ms * 100 / (100–40) **= 1.813 ms.**
- 21.33 ms + 1.813 ms **= 23.143 ms.**

Taking into account the time slices, the actual cycle time rounded up is **23.2 ms.**

Calculating the longest reaction time

- Longest reaction time
  23.2 ms * 2 = 46.4 ms.
- Delay of inputs and outputs
  - The maximum input delay of the digital input module SM 421; DI 32xDC 24 V is 4.8 ms per channel
  - The output delay of the digital output module SM 422; DO 16xDC 24 V/2A is negligible.
  - Analog input module SM 431; AI 8x13 bits was configured for 50 Hz interference frequency suppression. This results in a conversion time of 25 ms per channel. As eight channels are active, a cycle time of the analog output module of 200 ms results.
  - Analog output module SM 432; AO 8x13 bits is configured for operation in the measuring range 0 ...10V. This results in a conversion time of 0.3 ms per channel. As eight channels are active, a cycle time of 2.4 ms results. The transient time of a resistive load of 0.1 ms must be added to this. The result is an analog output response time of 2.5 ms.
- All the components are installed in the central unit, so DP cycle times can be ignored.
- Use case 1: The system sets a digital output channel after a digital input signal is read in. The result is a reaction time of:

  Reaction time = 46.4 ms + 4.8 ms = 51.2 ms.
- Use case 2: The system reads in and outputs an analog value. The result is a reaction time of:

  Reaction time = 46.4 ms + 200 ms + 2.5 ms = 248.9 ms.

16.8 Interrupt reaction time

Definition of interrupt reaction time

The interrupt reaction time is the time from the first occurrence of an interrupt signal to the call of the first instruction in the interrupt OB.

General rule: Higher-priority interrupts take precedence. This means the interrupt reaction time is increased by the program execution time of the higher-priority interrupt OBs, and by previous interrupt OBs of the same priority which have not yet been processed (queue).

Calculating the interrupt response time

Minimum interrupt reaction time of the CPU
+ minimum interrupt reaction time of the signal modules
+ DP cycle time on PROFIBUS–DP

= Shortest interrupt reaction time

Maximum interrupt reaction time of the CPU
+ maximum interrupt reaction time of the signal modules
+ 2 * DP cycle time on PROFIBUS–DP

= Longest interrupt reaction time

Process and diagnostic interrupt reaction times of the CPUs

Table 16-13 Process and interrupt reaction times; maximum interrupt reaction time without communication

CPU	Hardware interrupt reaction times		Diagnostic interrupt reaction times	
	min.	max.	min.	max.
412-3H stand-alone mode	366 μs	572 μs	354 μs	563 μs
412-3H redundant	370 μs	1143 μs	620 μs	982 μs
414-4H stand-alone mode	231 μs	361 μs	225 μs	356 μs
414-4H redundant	464 μs	726 μs	366 μs	592 μs
417-4H stand-alone mode	106 μs	158 μs	104 μs	167 μs
417-4H redundant	234 μs	336 μs	185 μs	294 μs

Increasing the maximum interrupt reaction time with communication

The maximum interrupt reaction time increases when communication functions are active. The increase is calculated with the following formula:

CPU 41x–4H t_v = 100 μs + 1000 μs × n%, significant extension possible where n = cycle load due to communication

Signal modules

The process interrupt reaction time of signal modules is made up as follows:

- Digital input modules

  Process interrupt reaction time = internal interrupt processing time + input delay

  For information on times, refer to the data sheet of the relevant digital input module.

- Analog input modules

  Process interrupt reaction time = internal interrupt processing time + conversion time

  The internal interrupt processing time of the analog input modules is negligible. For information on conversion times, refer to the data sheet of the relevant analog input module.

The diagnostic interrupt reaction time of the signal modules is the time from detection of a diagnostic event by the signal module to the triggering of the diagnostic interrupt by the module. This time is negligible.

Process interrupt handling

Process interrupt processing is initiated with the call of process interrupt OB 4x. Higher-priority interrupts interrupt process interrupts processing, and direct access to the I/O is made when the instruction is executed. After the process interrupt has been processed, the system either resumes cyclic program execution, or calls and processes interrupt OBs of the same or lower priority.

16.9 Example of calculation of the interrupt reaction time

Elements of the interrupt reaction time

As a reminder: The process interrupt reaction time is made up of:

- the process interrupt reaction time of the CPU and
- the process interrupt reaction time of the signal module.
- 2 × DP cycle time on PROFIBUS DP

Example: You have installed a 417-4H CPU and four digital modules in the central unit. One digital input module is the SM 421; DI 16xUC 24/60 V; with process and diagnostic interrupts. In the CPU and SM parameters, you have only enabled the process interrupt. You have no time-driven processing, diagnostics or error handling. For the digital input module you have configured an input delay of 0.5 ms. No actions at the cycle checkpoint are required. You have set a communication load of 20 % for the cycle.

Calculation

The process interrupt reaction time for the example is derived from the following times:

- Process interrupt reaction time of CPU 417-4H: Approx. 0.6 ms (mean value in redundant mode)
- Extension due to communication according to the description in Section Interrupt reaction time (Page 314):

100 µs + 1000 µs × 20% = 300 µs = 0.3 ms

- Process interrupt reaction time of SM 421; DI 16 x UC 24/60 V:
  - \- Internal interrupt processing time: 0.5 ms
  - \- Input delay: 0.5 ms
- The DP cycle time on the PROFIBUS-DP is irrelevant, because the signal modules are installed in the central unit.

The process interrupt reaction time is produced from the sum of the listed times:

Hardware interrupt reaction time = 0.6 ms +0.3 ms + 0.5 ms + 0.5 ms = approx. 1.9 ms.

This calculated process interrupt reaction time is the time between detection of a signal at the digital input and the call of the first instruction in OB 4x.

16.10 Reproducibility of delay and watchdog interrupts

Definition of "reproducibility"

Time-delay interrupt:

The period that expires between the call of the first instruction in the interrupt OB and the programmed time of interrupt.

Cyclic interrupt:

The fluctuation of the time interval between two successive calls, measured between the first instructions of the interrupt OB.

Reproducibility

The following table contains the reproducibility of time-delay and cyclic interrupts of the CPUs.

Table 16-14 Reproducibility of time-delay and cyclic interrupts of the CPUs

Module	Reproducibility	
	Time-delay interrupt	Cyclic interrupt
CPU 412-3H stand-alone mode	-499 µs / +469 µs	-315 µs / +305 µs
CPU 412-3H redundant	-557 µs / +722 µs	-710 µs / +655 µs
CPU 414-4H stand-alone mode	-342 µs / +386 µs	-242 µs / +233 µs
CPU 414-4H redundant	-545 µs / +440 µs	-793 µs / +620 µs
CPU 417-4H stand-alone mode	-311 µs / +277 µs	-208 µs / +210 µs
CPU 417-4H redundant	-453 µs / +514 µs	-229 µs / +289 µs

These times only apply if the interrupt can actually be executed at this time and if not interrupted, for example, by higher-priority interrupts or queued interrupts of equal priority.

Technical data 17

17.1 Technical specifications of the CPU 412–3H; (6ES7412 3HJ14 0AB0)

CPU and product version	
MLFB	6ES7412–3HJ14–0AB0
• Firmware version	V 4.5
Associated programming package	STEP 7 V 5.3 SP2 or higher with hardware update

Memory	
Work memory	
• Integrated	512 KB for code 256 KB for data
Load memory	
• Integrated	256 KB of RAM
• Expandable FEPROM	With memory card (FLASH) 1 MB up to 64 MB
• Expandable RAM	With memory card (RAM) 256 KB up to 64 MB
Backup with battery	Yes, all data

Processing times	
Processing times for	
• Bit instructions	75 ns
• Word instructions	75 ns
• Fixed-point math	75 ns
• Floating-point math	225 ns

Timers/counters and their retentivity	
S7 counters	2048
• Retentivity selectable	from C 0 to C 2047
• Preset	from C 0 to C 7
• Count range	0 to 999
IEC counters	Yes
• Type	SFB
S7 timers	2048
• Retentivity selectable	from T 0 to T 2047
• Preset	No retentive timers
• Time range	10 ms to 9990 s
IEC timers	Yes
• Type	SFB

Data areas and their retentivity	
Total retentive data area (incl. bit memory, timers, counters)	Total work and load memory (with backup battery)
Bit memory	8 KB
• Retentivity selectable	from MB 0 to MB 8191
• Preset retentivity	from MB 0 to MB 15
Clock memory bits	8 (1 memory byte)
Data blocks	Maximum 4095 (DB 0 reserved) Band of numbers 1 - 4095
• Size	Max. 64 KB
Local data (selectable)	Max. 16 KB
• Preset	8 KB

Blocks	
OBs	See instruction list
• Size	Max. 64 KB
Nesting depth	
• Per priority class	24
• Additional in an error OB	1
SDBs	maximum 512
FBs	Maximum 2048 Band of numbers 0 - 2047
• Size	Max. 64 KB
FCs	Maximum 2048 Band of numbers 0 - 2047
• Size	Max. 64 KB

Address areas (inputs/outputs)	
Total I/O address area	8 KB/8 KB
• Distributed	including diagnostic addresses, addresses for I/O interface modules, etc
MPI/DP interface	2 KB/2 KB
Process image	8 KB / 8 KB (selectable)
• Preset	256 bytes/256 bytes
• Number of process image partitions	Max. 15
• Consistent data	Max. 244 bytes
Access to consistent data in the process image	Yes
Digital channels	Max. 65536/ Max. 65536
• Central	Max. 65536/ Max. 65536
Analog channels	Max. 4096/ Max. 4096
• Central	Max. 4096/ Max. 4096

Configuration	
Central units/expansion units	Max. 1/21
Multicomputing	No
Number of plug-in IMs (total)	Max. 6
• IM 460	Max. 6
• IM 463–2	Max. 4, in stand-alone mode only
Number of DP masters	
• Integrated	1
• Via CP 443–5 Ext.	Max. 10
Operable FMs and CPs	
• FM, CP (point-to-point) see Appendix Function modules and communication processors supported by the S7-400H (Page 373).	Limited by the number of slots and the number of connections
• CP 441	Limited by the number of connections, maximum of 30
• PROFIBUS and Ethernet CPs including CP 443–5 Extended	Maximum 14, of which max. 10 CPs as DP masters
Connectable OPs	15, 8 of these with message processing

Time	
Clock (real-time clock)	Yes
• Buffered	Yes
• Resolution	1 ms
Maximum deviation per day	
• Power off (backed up)	1.7 s
• Power on (not backed up)	8.6 s
Operating hours counter	8
• Number/number range	0 to 7
• Range of values	0 to 32767 hours
• Granularity	1 hour
• Retentive	Yes
Clock synchronization	Yes
• In AS, on MPI and DP	As master or slave
Time difference in the system with synchronization via MPI	Max. 200 ms

S7 message functions	
Number of stations that can log on for message functions (for example WIN CC or SIMATIC OP)	Max. 8
Block-related messages	Yes
• Simultaneously active Alarm_S/SQ blocks and Alarm_D/DQ blocks	Max. 100
Alarm_8 blocks	Yes
• Number of communication jobs for ALARM_8 blocks **and** blocks for S7 communication (selectable)	Max. 600
• Preset	300
Process control messages	Yes
Number of archives that can log on simultaneously (SFB 37 AR_SEND)	16

Test and commissioning functions	
Status/modify variable	Yes
• Variable	Inputs/outputs, bit memory, DB, distributed inputs/outputs, timers, counters
• Number of variables	Max. 70
Force	Yes
• Variable	Inputs/outputs, bit memory, distributed inputs/outputs
• Number of variables	Max. 256
Status LED	Yes, FRCE-LED
Status block	Yes
Single step	Yes
Number of breakpoints	4
Diagnostic buffer	Yes
• Number of entries	Maximum 3200 (selectable)
• Preset	120

Communication	
PG/OP communication	Yes
Routing	Yes
S7 communication	Yes
• User data per job	Max. 64 KB
• Of which consistent	1 variable (462 bytes)
S7 basic communication	No
Global data communication	No
S5-compatible communication	Using FC AG_SEND and AG_RECV, max. via 10 CP 443–1 or 443–5 modules
• User data per job	Max. 8 KB
• Of which consistent	240 bytes
Number of simultaneous AG_SEND/AG_RECV jobs	Max. 24/24, see CP manual
Standard communication (FMS)	Yes, via CP and loadable FB
Number of connection resources for S7 connections via all interfaces and CPs	16, incl. one each reserved for PG and OP

Interfaces
Do not configure the CPU as a DP slave.

1. Interface	
Type of interface	Integrated
Physical properties	RS-485/PROFIBUS and MPI
Isolated	Yes
Interface power supply (15 V DC to 30 V DC)	Max. 150 mA
Number of connection resources	MPI: 16, DP: 16

Functionality	
• MPI	Yes
• PROFIBUS DP	DP master

1. Interface in MPI mode	
Services	
• PG/OP communication	Yes
• Routing	Yes
• S7 communication	Yes
• Global data communication	No
• S7 basic communication	No
• Transmission rates	Max. 12 Mbps

1. Interface in DP master mode	
Services	
• PG/OP communication	Yes
• Routing	Yes
• S7 communication	Yes
• Global data communication	No
• S7 basic communication	No
• Constant bus cycle time	No
• SYNC/FREEZE	No
• Enable/disable DP slaves	No
• Direct data exchange (slave-to-slave communication)	No
Transmission rates	Max. 12 Mbps
Number of DP slaves	Max. 32
Number of slots per interface	maximum 544
Address area	Maximum 2 KB inputs / 2 KB outputs

1. Interface in DP master mode	
User data per DP slave	Maximum 244 Maximum 244 bytes inputs Maximum 244 bytes outputs Maximum 244 slots Maximum 128 bytes per slot
Note: • The total sum of the input bytes across all slots may not exceed 244. • The total sum of the output bytes across all slots may not exceed 244. • The address range of the interface (maximum 2 KB inputs / 2 KB outputs) must not be exceeded in total across all 32 slaves.	

2. and 3rd interface	
Type of interface	Plug-in synchronization module (fiber-optic cable)
Usable interface module	Synchronization module IF 960 (only in redundant mode; in stand-alone mode the interface is free/covered)
Length of the synchronization cable	Max. 10 m, can only be operated with synchronization module 6ES7960-1AA04-0XA0

Programming	
Programming language	LAD, FBD, STL, SCL, CFC, Graph, HiGraph®
Instruction set	See instruction list
Nesting levels	8
System functions (SFC)	See instruction list
Number of simultaneously active SFCs per chain	
• SFC 59 "RD_REC"	8
• SFC 58 "WR_REC"	8
• SFC55 "WR_PARM"	8
• SFC57 "PARM_MOD"	1
• SFC56 "WR_DPARM"	2
• SFC13 "DPNRM_DG"	8
• SFC51 "RDSYSST"	8
• SFC103 "DP_TOPOL"	1
The total number of active SFCs on all external chains may be four times more than on one single chain.	
System function blocks (SFB)	See instruction list
Number of simultaneously active SFBs per chain	
• SFB52 "RDREC"	8
• SFB53 "WRREC"	8
The total number of active SFBs on all external chains may be four times more than on one single chain.	
User program protection	Password protection
Access to consistent data in the process image	Yes

CiR synchronization time (in stand-alone mode)	
Base load	150 ms
Time per I/O byte	40 μs

Dimensions	
Mounting dimensions W x H x D (mm)	50 x 290 x 219
Slots required	2
Weight	Approx. 0.990 kg

Voltages, currents	
Current consumption from the S7-400 bus (5 V DC)	Typ. 1.2 A Max. 1.5 A
Current consumption from S7-400 bus (24 V DC) The CPU does not consume any current at 24 V, it only makes this voltage available on the MPI/DP interface.	Total current consumption of the components connected to the MPI/DP interfaces, however with a maximum of 150 mA per interface
Current output to DP interface (5 V DC)	Max. 90 mA
Backup current	Typically 190 μA (up to 40° C) Maximum 660 μA
Maximum backup time	See *Module Specifications* reference manual, Section 3.3.
Feed of external backup voltage to the CPU	5 V to 15 V DC
Power loss	Typ. 6.0 W

17.2 Technical specifications of the CPU 414–4H; (6ES7414-4HM14-0AB0)

CPU and product version	
MLFB	6ES7414–4HM14–0AB0
• Firmware version	V 4.5
Associated programming package	STEP 7 V 5.3 SP2 or higher with hardware update

Memory	
Work memory	
• Integrated	1400 KB for code 1400 KB for data
Load memory	
• Integrated	256 KB of RAM
• Expandable FEPROM	With memory card (FLASH) 1 MB up to 64 MB
• Expandable RAM	With memory card (RAM) 256 KB up to 64 MB
Backup with battery	Yes, all data

Processing times	
Processing times for	
• Bit instructions	45 ns
• Word instructions	45 ns
• Fixed-point math	45 ns
• Floating-point math	135 ns

Timers/counters and their retentivity	
S7 counters	2048
• Retentivity selectable	from C 0 to C 2047
• Preset	from C 0 to C 7
• Count range	0 to 999
IEC counters	Yes
• Type	SFB
S7 timers	2048
• Retentivity selectable	from T 0 to T 2047
• Preset	No retentive timers
• Time range	10 ms to 9990 s
IEC timers	Yes
• Type	SFB

Data areas and their retentivity	
Total retentive data area (incl. bit memory, timers, counters)	Total work and load memory (with backup battery)
Bit memory	8 KB
• Retentivity selectable	from MB 0 to MB 8191
• Preset retentivity	from MB 0 to MB 15
Clock memory bits	8 (1 memory byte)
Data blocks	Maximum 4095 (DB 0 reserved) Band of numbers 1 - 4095
• Size	Max. 64 KB
Local data (selectable)	Max. 16 KB
• Preset	8 KB

Blocks	
OBs	See instruction list
• Size	Max. 64 KB
Nesting depth	
• Per priority class	24
• Additional in an error OB	1
SDBs	maximum 512
FBs	Maximum 2048 Band of numbers 0 - 2047
• Size	Max. 64 KB
FCs	Maximum 2048 Band of numbers 0 - 2047
• Size	Max. 64 KB

Address areas (inputs/outputs)	
Total I/O address area	8 KB/8 KB
• Distributed	including diagnostic addresses, addresses for I/O interface modules, etc.
MPI/DP interface	2 KB/2 KB
DP interface	6 KB/6 KB
Process image	8 KB / 8 KB (selectable)
• Preset	256 bytes/256 bytes
• Number of process image partitions	Max. 15
• Consistent data	Max. 244 bytes

Address areas (inputs/outputs)	
Access to consistent data in the process image	Yes
Digital channels	Max. 65536/ Max. 65536
• Central	Max. 65536/ Max. 65536
Analog channels	Max. 4096/ Max. 4096
• Central	Max. 4096/ Max. 4096

Configuration	
Central units/expansion units	Max. 1/21
Multicomputing	No
Number of plug-in IMs (total)	Max. 6
• IM 460	Max. 6
• IM 463–2	Max. 4, in stand-alone mode only
Number of DP masters	
• Integrated	2
• Via CP 443–5 Ext.	Max. 10
Operable FMs and CPs	
• FM, CP (point-to-point) see Appendix Function modules and communication processors supported by the S7-400H (Page 373).	Limited by the number of slots and the number of connections
• CP 441	Limited by the number of connections, maximum of 30
• PROFIBUS and Ethernet CPs including CP 443–5 Extended	Maximum 14, of which max. 10 CPs as DP masters
Connectable OPs	31, 8 of these with message processing

Time	
Clock	Yes
• Buffered	Yes
• Resolution	1 ms
Maximum deviation per day	
• Power off (backed up)	1.7 s
• Power on (not backed up)	8.6 s
Operating hours counter	8
• Number	0 to 7
• Range of values	0 to 32767 hours
• Granularity	1 hour
• Retentive	Yes

Time	
Clock synchronization	Yes
• In AS, on MPI and DP	As master or slave
Time difference in the system with synchronization via MPI	Max. 200 ms

S7 message functions	
Number of stations that can log on for message functions (for example WIN CC or SIMATIC OP)	Max. 8
Block-related messages	Yes
• Simultaneously active Alarm_S/SQ blocks and Alarm_D/DQ blocks	Max. 100
Alarm_8 blocks	Yes
• Number of communication jobs for ALARM_8 blocks **and** blocks for S7 communication (selectable)	Max. 1200
• Preset	900
Process control messages	Yes
Number of archives that can log on simultaneously (SFB 37 AR_SEND)	16

Test and commissioning functions	
Status/modify variable	Yes
• Variable	Inputs/outputs, bit memory, DB, distributed inputs/outputs, timers, counters
• Number of variables	Max. 70
Force	Yes
• Variable	Inputs/outputs, bit memory, distributed inputs/outputs
• Number of variables	Max. 256
Status LED	Yes, FRCE-LED
Status block	Yes
Single step	Yes
Number of breakpoints	4
Diagnostic buffer	Yes
• Number of entries	Maximum 3200 (selectable)
• Preset	120

Communication	
PG/OP communication	Yes
Routing	Yes
S7 communication	Yes
• User data per job	Max. 64 KB
• Of which consistent	1 variable (462 bytes)
S7 basic communication	No
Global data communication	No
S5-compatible communication	Using FC AG_SEND and AG_RECV, max. via 10 CP 443–1 or 443–5 modules
• User data per job	Max. 8 KB
• Of which consistent	240 bytes
Number of simultaneous AG_SEND/AG_RECV jobs	Max. 24/24, see CP manual
Standard communication (FMS)	Yes (via CP and loadable FB)
Number of connection resources for S7 connections via all interfaces and CPs	32, incl. one each reserved for PG and OP

Interfaces
Do not configure the CPU as a DP slave.

1. Interface	
Type of interface	Integrated
Physical properties	RS 485/Profibus
Isolated	Yes
Interface power supply (15 V DC to 30 V DC)	Max. 150 mA
Number of connection resources	MPI: 32, DP: 32

Functionality	
• MPI	Yes
• PROFIBUS DP	DP master

1. Interface in MPI mode	
Services	
• PG/OP communication	Yes
• Routing	Yes
• S7 communication	Yes
• Global data communication	No
• S7 basic communication	No
• Transmission rates	Max. 12 Mbps

1. Interface in DP master mode	
• Services	
• PG/OP communication	Yes
• Routing	Yes
• S7 communication	Yes
• Global data communication	No
• S7 basic communication	No
• Constant bus cycle time	No
• SYNC/FREEZE	No
• Enable/disable DP slaves	No
• Direct data exchange (slave-to-slave communication)	No
• Transmission rates	Max. 12 Mbps
• Number of DP slaves	Max. 32
• Number of slots per interface	maximum 544
• Address area	Maximum 2 KB inputs / 2 KB outputs
• User data per DP slave	Maximum 244 bytes Maximum 244 bytes inputs, Maximum 244 bytes outputs, Maximum 244 slots Maximum 128 bytes per slot
Note: • The total sum of the input bytes across all slots may not exceed 244. • The total sum of the output bytes across all slots may not exceed 244. • The address range of the interface (maximum 2 KB inputs / 2 KB outputs) must not be exceeded in total across all 32 slaves.	

2. Interface	
Type of interface	Integrated
Physical properties	RS 485/Profibus
Isolated	Yes
Interface power supply (15 V DC to 30 V DC)	Max. 150 mA
Number of connection resources	16

Functionality	
• PROFIBUS DP	DP master

2. Interface in DP master mode	
Services	
• PG/OP communication	Yes
• Routing	Yes
• S7 communication	Yes
• Global data communication	No
• S7 basic communication	No
• Constant bus cycle time	No
• SYNC/FREEZE	No
• Enable/disable DP slaves	No
• Direct data exchange (slave-to-slave communication)	No
• Transmission rates	Up to 12 Mbps
• Number of DP slaves	Max. 96
• Number of slots per interface	Maximum 1632
• Address area	Maximum 6 KB inputs / 6 KB outputs
• User data per DP slave	Maximum 244 bytes Maximum 244 bytes inputs, Maximum 244 bytes outputs, Maximum 244 slots Maximum 128 bytes per slot
Note: • The total sum of the input bytes across all slots may not exceed 244. • The total sum of the output bytes across all slots may not exceed 244. • The address range of the interface (maximum 6 KB inputs / 6 KB outputs) must not be exceeded in total across all 96 slaves.	

3. and 4th interface	
Type of interface	Plug-in synchronization module (fiber-optic cable)
Usable interface module	Synchronization module IF 960 (only in redundant mode; in stand-alone mode the interface is free/covered)
Length of the synchronization cable	Max. 10 km

Programming	
Programming language	LAD, FBD, STL, SCL, CFC, Graph, HiGraph®
Instruction set	See instruction list
Nesting levels	8
System functions (SFC)	See instruction list
Number of simultaneously active SFCs per chain	
• SFC 59 "RD_REC"	8
• SFC 58 "WR_REC"	8
• SFC55 "WR_PARM"	8
• SFC57 "PARM_MOD"	1
• SFC56 "WR_DPARM"	2
• SFC13 "DPNRM_DG"	8
• SFC51 "RDSYSST"	8
• SFC103 "DP_TOPOL"	1
The total number of active SFCs on all external chains may be four times more than on one single chain.	
System function blocks (SFB)	See instruction list
Number of simultaneously active SFBs per chain	
• SFB52 "RDREC"	8
• SFB53 "WRREC"	8
The total number of active SFBs on all external chains may be four times more than on one single chain.	
User program protection	Password protection
Access to consistent data in the process image	Yes

CiR synchronization time (in stand-alone mode)	
Base load	100 ms
Time per I/O byte	25 µs

Dimensions	
Mounting dimensions W x H x D (mm)	50 x 290 x 219
Slots required	2
Weight	Approx. 0.995 kg

Voltages, currents	
Current consumption from S7–400 bus (5 V DC)	Typ. 1.4 A Max. 1.7 A
Current consumption from S7-400 bus (24 V DC) The CPU does not consume any current at 24 V, it only makes this voltage available on the MPI/DP interface.	Total current consumption of the components connected to the MPI/DP interfaces, however a maximum of 150 mA per interface
Current output to DP interface (5 V DC)	Max. 90 mA
Backup current	Typically 190 µA (up to 40° C) Maximum 660 µA
Maximum backup time	See *Module Specifications* reference manual, Section 3.3.
Feed of external backup voltage to the CPU	5 V to 15 V DC
Power loss	Typ. 7.0 W

17.3 Technical specifications of the CPU 417–4H; (6ES7417-4HT14-0AB0)

CPU and product version	
MLFB	6ES7417–4HT14–0AB0
• Firmware version	V 4.5
Associated programming package	STEP 7 V 5.3 SP2 or higher with hardware update

Memory	
Work memory	
• Integrated	15 MB for code 15 MB for data
Load memory	
• Integrated	256 KB of RAM
• Expandable FEPROM	With memory card (FLASH) 1 MB up to 64 MB
• Expandable RAM	With memory card (RAM) 256 KB up to 64 MB
Backup with battery	Yes, all data

Processing times	
Processing times for	
• Bit instructions	18 ns
• Word instructions	18 ns
• Fixed-point math	18 ns
• Floating-point math	54 ns

Timers/counters and their retentivity	
S7 counters	2048
• Retentivity selectable	from C 0 to C 2047
• Preset	from C 0 to C 7
• Count range	0 to 999
IEC counters	Yes
• Type	SFB
S7 timers	2048
• Retentivity selectable	from T 0 to T 2047
• Preset	No retentive timers
• Time range	10 ms to 9990 s
IEC timers	Yes
• Type	SFB

Data areas and their retentivity	
Total retentive data area (incl. bit memory, timers, counters)	Total work and load memory (with backup battery)
Bit memory	16 KB
• Retentivity selectable	from MB 0 to MB 16383
• Preset retentivity	from MB 0 to MB 15
Clock memory bits	8 (1 memory byte)
Data blocks	Maximum 8191 (DB 0 reserved) Band of numbers 1 to 8191
• Size	Max. 64 KB
Local data (selectable)	Max. 64 KB
• Preset	32 KB

Blocks	
OBs	See instruction list
• Size	Max. 64 KB
Nesting depth	
• Per priority class	24
• Additional in an error OB	2
SDBs	maximum 512
FBs	Maximum 6144 Band of numbers 0 - 6143
• Size	Max. 64 KB
FCs	Maximum 6144 Band of numbers 0 - 6143
• Size	Max. 64 KB

Address areas (inputs/outputs)	
Total I/O address area	16 KB/16 KB
• Distributed	incl. diagnostics addresses, addresses for I/O interface modules, etc
MPI/DP interface	2 KB/2 KB
DP interface	8 KB/8 KB
Process image	16 KB/16 KB (programmable)
• Preset	1024 bytes/1024 bytes
• Number of process image partitions	Max. 15
• Consistent data	Max. 244 bytes

Address areas (inputs/outputs)	
Access to consistent data in the process image	Yes
Digital channels	Max. 131072/ Max. 131072
• Central	Max. 131072/ Max. 131072
Analog channels	Max. 8192/ Max. 8192
• Central	Max. 8192/ Max. 8192

Configuration	
Central units/expansion units	Max. 1/21
Multicomputing	No
Number of plug-in IMs (total)	Max. 6
• IM 460	Max. 6
• IM 463–2	Max. 4, in stand-alone mode only
Number of DP masters	
• Integrated	2
• Via CP 443–5 Ext.	Max. 10
Number of plug-in S5 modules via adapter casing (in the central unit)	None
Operable function modules and communication processors	
• FM, CP (point-to-point) see Appendix Function modules and communication processors supported by the S7-400H (Page 373).	Limited by the number of slots and the number of connections
• CP 441	Limited by the number of connections, maximum of 30
• PROFIBUS and Ethernet CPs including CP 443–5 Extended	Maximum 14, of which max. 10 CPs as DP masters
Connectable OPs	63, 16 of these with message processing

Time	
Clock	Yes
• Buffered	Yes
• Resolution	1 ms
Maximum deviation per day	
• Power off (backed up)	1.7 s
• Power on (not backed up)	8.6 s

Time	
Operating hours counter	8
• Number	0 to 7
• Range of values	0 to 32767 hours
• Granularity	1 hour
• Retentive	Yes
Clock synchronization	Yes
• In AS, on MPI and DP	As master or slave
Time difference in the system with synchronization via MPI	Max. 200 ms

S7 message functions	
Number of stations that can log on for message functions (for example WIN CC or SIMATIC OP)	Max. 16
Block-related messages	Yes
• Simultaneously active Alarm_S/SQ blocks and Alarm_D/DQ blocks	Max. 200
Alarm_8 blocks	Yes
• Number of communication jobs for ALARM_8 blocks **and** blocks for S7 communication (selectable)	Max. 10000
• Preset	1200
Process control messages	Yes
Number of archives that can log on simultaneously (SFB 37 AR_SEND)	64

Test and commissioning functions	
Status/modify variable	Yes
• Variable	Inputs/outputs, bit memory, DB, distributed inputs/outputs, timers, counters
• Number of variables	Max. 70
Force	Yes
• Variable	Inputs/outputs, bit memory, distributed inputs/outputs
• Number of variables	maximum 512
Status LED	Yes, FRCE-LED
Status block	Yes
Single step	Yes
Number of breakpoints	4
Diagnostic buffer	Yes
• Number of entries	Maximum 3200 (selectable)
• Preset	120

Communication	
PG/OP communication	Yes
Routing	Yes
Number of connection resources for S7 connections via all interfaces and CPs	64, incl. one each reserved for PG and OP
S7 communication	Yes
• User data per job	64 bytes
• Of which consistent	1 variable (462 bytes)
Global data communication	No
S7 basic communication	No
S5-compatible communication	Using FC AG_SEND and AG_RECV, max. via 10 CP 443–1 or 443–5 modules
• User data per job	Max. 8 KB
• Of which consistent	240 bytes
Number of simultaneous AG_SEND/AG_RECV jobs	Max. 64/64, see CP manual
Standard communication (FMS)	Yes (by means of CP and loadable FC)
Number of connection resources for S7 connections via all interfaces and CPs	64, incl. one each reserved for PG and OP

Interfaces
Do not configure the CPU as a DP slave.

1. Interface	
Type of interface	Integrated
Physical properties	RS 485/Profibus
Isolated	Yes
Interface power supply (15 V DC to 30 V DC)	Max. 150 mA
Number of connection resources	MPI: 44, DP: 32 a diagnostic repeater in the chain reduces the number of connection resources by 1

Functionality	
• MPI	Yes
• PROFIBUS DP	DP master

1. Interface in MPI mode	
• Services	
• PG/OP communication	Yes
• Routing	Yes
• S7 communication	Yes
• Global data communication	No
• S7 basic communication	No
• Transmission rates	Max. 12 Mbps

1. Interface in DP master mode	
Services	
• PG/OP communication	Yes
• Routing	Yes
• S7 communication	Yes
• Global data communication	No
• S7 basic communication	No
• Constant bus cycle time	No
• SYNC/FREEZE	No
• Enable/disable DP slaves	No
• Direct data exchange (slave-to-slave communication)	No
Transmission rates	Max. 12 Mbps
Number of DP slaves	Max. 32
Number of slots per interface	maximum 544
Address area	Maximum 2 KB inputs / 2 KB outputs
User data per DP slave	Maximum 244 bytes Maximum 244 bytes inputs, Maximum 244 bytes outputs, Maximum 244 slots Maximum 128 bytes per slot
Note: • The total sum of the input bytes across all slots may not exceed 244. • The total sum of the output bytes across all slots may not exceed 244. • The address range of the interface (maximum 2 KB inputs / 2 KB outputs) must not be exceeded in total across all 32 slaves.	

2. Interface	
Type of interface	Integrated
Physical properties	RS 485/Profibus
Isolated	Yes
Interface power supply (15 V DC to 30 V DC)	Max. 150 mA
Number of connection resources	32, a diagnostic repeater in the chain reduces the number of connection resources by 1

Functionality	
• PROFIBUS DP	DP master

2. Interface in DP master mode	
Services	
• PG/OP communication	Yes
• Routing	Yes
• S7 communication	Yes
• Global data communication	No
• S7 basic communication	No
• Constant bus cycle time	No
• SYNC/FREEZE	No
• Enable/disable DP slaves	No
• Direct data exchange (slave-to-slave communication)	No
Transmission rates	Max. 12 Mbps
Number of DP slaves	Max. 125
Number of slots per interface	maximum 2173
Address area	Maximum 8 KB inputs / 8 KB outputs
User data per DP slave	Maximum 244 bytes Maximum 244 bytes inputs, Maximum 244 bytes outputs, Maximum 244 slots Maximum 128 bytes per slot
Note: • The total sum of the input bytes across all slots may not exceed 244. • The total sum of the output bytes across all slots may not exceed 244. • The address range of the interface (maximum 8 KB inputs / 8 KB outputs) must not be exceeded in total across all 125 slaves.	

3. and 4th interface	
Type of interface	Plug-in synchronization module (fiber-optic cable)
Usable interface module	Synchronization module IF 960 (only in redundant mode; in stand-alone mode the interface is free/covered)
Length of the synchronization cable	Max. 10 km

Programming	
Programming language	LAD, FBD, STL, SCL, CFC, Graph, HiGraph®
Instruction set	See instruction list
Nesting levels	8
System functions (SFC)	See instruction list
Number of simultaneously active SFCs per chain	
• SFC 59 "RD_REC"	8
• SFC 58 "WR_REC"	8
• SFC55 "WR_PARM"	8
• SFC57 "PARM_MOD"	1
• SFC56 "WR_DPARM"	2
• SFC13 "DPNRM_DG"	8
• SFC51 "RDSYSST"	8
• SFC103 "DP_TOPOL"	1
The total number of active SFCs on all external chains may be four times more than on one single chain.	
System function blocks (SFB)	See instruction list
Number of simultaneously active SFBs per chain	
• SFB52 "RDREC"	8
• SFB53 "WRREC"	8
The total number of active SFBs on all external chains may be four times more than on one single chain.	
User program protection	Password protection
Access to consistent data in the process image	Yes

CiR synchronization time (in stand-alone mode)	
Base load	60 ms
Time per I/O byte	10 μs

Dimensions	
Mounting dimensions W x H x D (mm)	50 x 290 x 219
Slots required	2
Weight	Approx. 0.995 kg

Voltages, currents	
Current consumption from S7–400 bus (5 V DC)	Typ. 1.5 A Max. 1.8 A
Current consumption from S7-400 bus (24 V DC) The CPU does not consume any current at 24 V, it only makes this voltage available on the MPI/DP interface.	Total current consumption of the components connected to the MPI/DP interfaces, however a maximum of 150 mA per interface
Current output to DP interface (5 V DC)	Max. 90 mA
Backup current	Typically 970 µA (up to 40° C) Maximum 1980 µA
Maximum backup time	See Module Data reference manual, section 3.3
Feed of external backup voltage to the CPU	5 V to 15 V DC
Power loss	Typ. 7.5 W

17.4 Technical specifications of the memory cards

Data

Name	Order No.	Current consumption at 5 V	Backup currents
MC 952 / 256 Kbytes / RAM	6ES7952-1AH00-0AA0	typ. 35 mA max. 80 mA	typ. 1 µA max. 40 µA
MC 952 / 1 MB / RAM	6ES7952-1AK00-0AA0	typ. 40 mA max. 90 mA	typ. 3 µA max. 50 µA
MC 952 / 2 MB / RAM	6ES7952-1AL00-0AA0	typ. 45 mA max. 100 mA	typ. 5 µA max. 60 µA
MC 952 / 4 MB / RAM	6ES7952-1AM00-0AA0	typ. 45 mA max. 100 mA	typ. 5 µA max. 60 µA
MC 952 / 8 MB / RAM	6ES7952-1AP00-0AA0	typ. 45 mA max. 100 mA	typ. 5 µA max. 60 µA
MC 952 / 16 MB / RAM	6ES7952-1AS00-0AA0	typ. 100 mA max. 150 mA	typ. 50 µA max. 125 µA
MC 952 / 64 MB / RAM	6ES7952-1AY00-0AA0	typ. 100 mA max. 150 mA	typ. 100 µA max. 500 µA
MC 952 / 1 Mbytes / 5V Flash	6ES7952-1KK00-0AA0	typ. 40 mA max. 90 mA	–
MC 952 / 2 Mbytes / 5V Flash	6ES7952-1KL00-0AA0	typ. 50 mA max. 100 mA	–
MC 952 / 4 Mbytes / 5V Flash	6ES7952-1KM00-0AA0	typ. 40 mA max. 90 mA	–
MC 952 / 8 Mbytes / 5V Flash	6ES7952-1KP00-0AA0	typ. 50 mA max. 100 mA	–
MC 952 / 16 Mbytes / 5V Flash	6ES7952-1KS00-0AA0	typ. 55 mA max. 110 mA	–
MC 952 / 32 Mbytes / 5V Flash	6ES7952-1KT00-0AA0	typ. 55 mA max. 110 mA	–
MC 952 / 64 Mbytes / 5V Flash	6ES7952-1KY00-0AA0	typ. 55 mA max. 110 mA	–
Dimensions WxHxD (in mm)		7.5 x 57 x 87	
Weight		Max. 35 g	
EMC protection		Provided by construction	

17.5 Runtimes of the FCs and FBs for redundant I/Os

Table 17-1 Runtimes of the blocks for redundant I/Os

Block	Runtime in stand-alone/single mode	Runtime in redundant mode
FC 450 RED_INIT Specifications are based on the startup	2 ms + 300 μs / configured module pairs The specification for a module pair is a mean value. The runtime may be < 300 μs for a few modules. For a large number of redundant modules the value may be > 300 μs.	-
FC 451 RED_DEPA	160 μs	360 μs
FB 450 RED_IN Called from the corresponding sequence level.	750 μs + 60 μs / module pair of the current TPA The specification for a module pair is a mean value. The runtime may be additionally increased if discrepancies occur resulting in passivation and logging to the diagnostics buffer. The runtime may also be increased by a depassivation carried out at the individual sequence levels of FB RED_IN. Depending on the number of modules in the sequence level, the depassivation may increase the runtime of the FB RED_IN by 0.4 ... 8 ms. An 8 ms increase can be expected in redundant operation of modules totaling more than 370 pairs of modules at a sequence level.	1000 μs +70 μs / module pair of the current TPA The specification for a module pair is a mean value. The runtime may be additionally increased if discrepancies occur resulting in passivation and logging to the diagnostics buffer. The runtime may also be increased by a depassivation carried out at the individual sequence levels of FB RED_IN. Depending on the number of modules in the sequence level, the depassivation may increase the runtime of the FB RED_IN by 0.4 ... 8 ms. An 8 ms increase can be expected in redundant operation of modules totaling more than 370 pairs of modules at a sequence level.
FB 451 RED_OUT Called from the corresponding sequence level.	650 μs +2 μs / module pair of the current TPA The specification for a module pair is a mean value. The runtime may be < 2 μs for a few modules. For a large number of redundant modules the value may be > 2 μs.	860 μs +2 μs / module pair of the current TPA The specification for a module pair is a mean value. The runtime may be < 2 μs for a few modules. For a large number of redundant modules the value may be > 2 μs.
FB 452 RED_DIAG	Called in OB 72: 160 μs Called in OB 82, 83, 85: 250 μs + 5 μs / configured module pairs Under extreme conditions the runtime of FB RED_DIAG is increased up to 1.5 ms. . This is the case when the working DB is 60 KB or larger and if there are interrupt trigger addresses that do not belong to the redundant I/O.	Called in OB 72: 360 μs Called in OB 82, 83, 85: 430 μs (basic load) + 6 μs / configured module pairs Under extreme conditions the runtime of FB RED_DIAG is increased up to 1.5 ms. . This is the case when the working DB is 60 KB or larger and if there are interrupt trigger addresses that do not belong to the redundant I/O.

Block	Runtime in stand-alone/single mode	Runtime in redundant mode
FB 453 RED_STATUS	160 μs + 4 μs/ configured module pairs * number of module pairs) The runtime depends on the random position of the module being searched for in the working DB. When a module address is not redundant, the entire working DB is searched. This results in the longest runtime of FB RED_STATUS. The number of module pairs is based either on all inputs (DI/AI) or all outputs (DO/AO).	350 μs +5 μs/ configured module pairs * number of module pairs) The runtime depends on the random position of the module being searched for in the working DB. When a module address is not redundant, the entire working DB is searched. This results in the longest runtime of FB RED_STATUS. The number of module pairs is based either on all inputs (DI/AI) or all outputs (DO/AO).

NOTICE
These are guide values, not absolute values. The actual value may deviate from these specifications in some cases. This overview is intended as a guide and should help you estimate how use of the RED_IO library may change the cycle time.

A Characteristic values of redundant automation systems

This appendix provides a brief introduction to the characteristic values of redundant automation systems, and shows the practical effects of redundant configurations, based on a selection of configurations.

You will find an overview of the MTBF of various SIMATIC products in the SIMATIC FAQs at:

http://support.automation.siemens.com

under entry ID 16818490

A.1 Basic concepts

The quantitative assessment of redundant automation systems is usually based on their reliability and availability parameters. These are described in detail below.

Reliability

Reliability refers to the capability of technical equipment to fulfill its function during its operating period. This is usually no longer the case if any of its components fails.

So a commonly used measure for reliability is the **MTBF** (**M**ean **T**ime **B**etween **F**ailure). This can be analyzed statistically based on the parameters of running systems, or by calculating the failure rates of the components used.

Reliability of modules

The reliability of SIMATIC components is extremely high as a consequence of extensive quality assurance measures in design and production.

Reliability of automation systems

The use of redundant modules considerably prolongs the MTBF of a system. The combination of integrated high-quality self-tests and error detection mechanisms of the S7-400H CPUs allows the detection and localization of virtually all errors.

The MTBF of an S7-400H is determined by the **MDT** (**M**ean **D**own **T**ime) of a system unit. This time is derived in essence from the error detection time plus the time required to repair or replace defective modules.

In addition to other measures, a CPU provides a self-test function with an adjustable test cycle time. The default test cycle time is 90 minutes. This time has an influence on the error detection time. The repair time usually required for a modular system such as the S7-400H is four hours.

Mean Down Time (MDT)

The MDT of a system is determined by the times outlined below:

- Time required to detect an error
- Time required to find the cause of an error
- Time required for troubleshooting and to restart the system

The system MDT is calculated based on the MDT of the various system components. The structure in which the components make up the system also forms part of the calculation.

Correlation between MDT and MTBF: MDT << MTBF

The MDT value is of the highest significance for the quality of system maintenance. The most important factors are:

- Qualified personnel
- Efficient logistics
- High-performance tools for diagnostics and error recognition
- A sound repair strategy

The figure below shows the dependency of the MDT on the times and factors mentioned above.

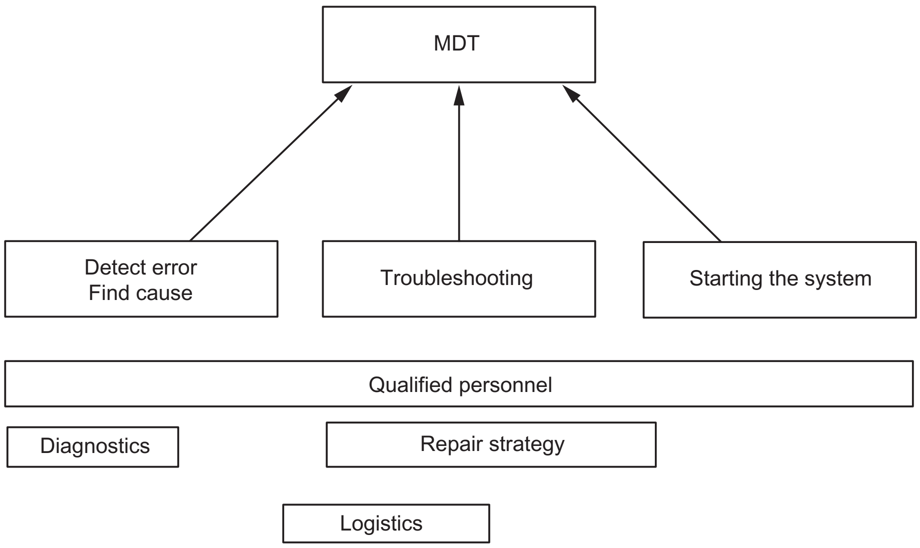


Figure A-1 MDT

The figure below shows the parameters included in the calculation of the MTBF of a system.

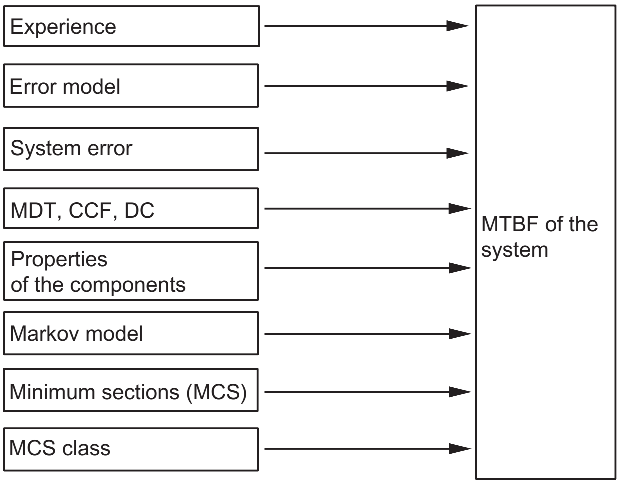


Figure A-2 MTBF

Requirements

This analysis assumes the following conditions:

- The failure rate of all components and all calculations is based on an average temperature of 40 °C.
- The system installation and configuration is free of errors.
- All replacement parts are available locally, in order to prevent extended repair times due to missing spare parts. This keeps the component MDT down to a minimum.
- The MDT of the various components is four hours. The system's MDT is calculated based on the MDT of the various components plus the system structure.
- The MTBF of the components conforms to the SN 29500 standard, which corresponds to MIL–HDBK 217–F.
- The calculations are made using the diagnostic coverage of each component.
- A CCF factor between 0.2 % and 2 % is assumed, depending on the system configuration.

Common Cause Failure (CCF)

The Common Cause Failure (CCF) is an error which is caused by one or more events which also lead to an error state on two or more separate channels or components in a system. A CCF leads to a system failure.

The CCF may be caused by one of the following factors:

- Temperature
- Humidity
- Corrosion
- Vibration and shock
- EMC interference
- Electrostatic discharge
- RF interference
- Unexpected sequence of events
- Operating errors

The CCF factor defines the ratio between the probability of the occurrence of a CCF and the probability of the occurrence of any other error.

Typical CCF factors range from 2% to 0.2 % in a system with identical components, and between 1% and 0.1% in a system containing different components.

Within the range stipulated in IEC 61508, a CCF factor between 0.02% and 5% is used to calculate the MTBF.

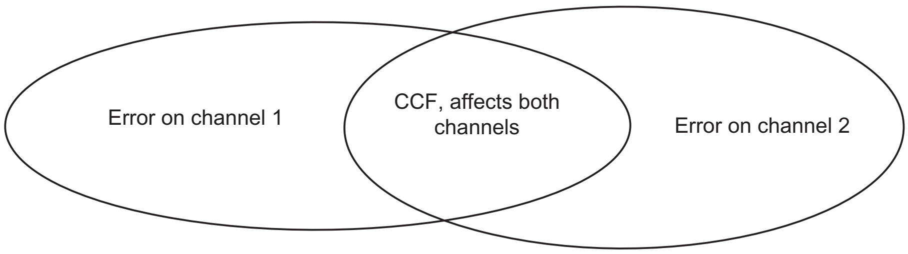


Figure A-3 Common Cause Failure (CCF)

Reliability of an S7-400H

The use of redundant modules prolongs the system MTBF by a very large factor. The integrated high-grade self-test and the test/message functions of the S7-400H CPUs enable the detection and localization of virtually all errors. The calculated diagnostic coverage is around 90%.

The reliability in stand-alone mode is described by the corresponding failure rate. This corresponds to the reciprocal value of the MTTF (Mean Time To Failure). The MTTF is equivalent to the MTBF, assuming an infinite repair time MDT. The failure rate of an S7-400H is calculated according to the SN29500 standard.

The reliability in redundant mode is described by the corresponding failure rate. This corresponds to the reciprocal value of the MTTF. Those combinations of failed components which cause a system failure form the minimum sections. The minimum sections are described individually by the Markov model.

Availability

Availability is the probability that a system is operable at a given point of time. This can be enhanced by means of redundancy, for example by using redundant I/O modules or multiple encoders at the same sampling point. Redundant components are arranged such that system operability is not affected by the failure of a single component. Here, again, an important element of availability is a detailed diagnostics display.

The availability of a system is expressed as a percentage. It is defined by the mean time between failure (MTBF) and the mean time to repair MTTR (MDT). The availability of a two-channel (1-of-2) H system can be calculated using the following formula:

$$V = \frac{MTBF_{1v2}}{MTBF_{1v2} + MDT} 100\%$$

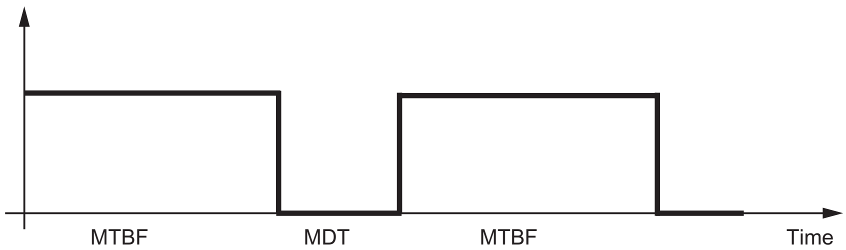


Figure A-4 Availability

A.2 Comparison of MTBF for selected configurations

The following sections compare systems with a centralized and distributed I/Os.

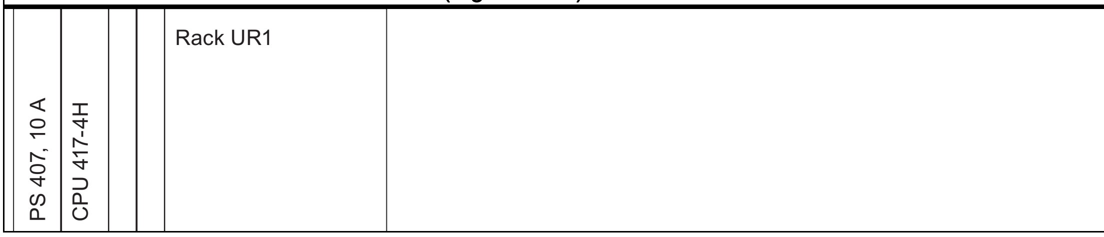
The following framework conditions are set for the calculation.

- MDT (Mean Down Time) 4 hours
- Ambient temperature 40 degrees
- Buffer voltage is safeguarded

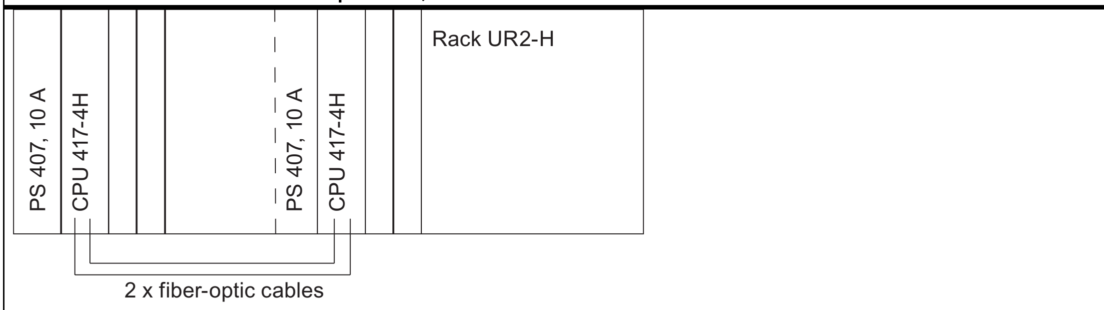
A.2.1 System configurations with centralized I/Os

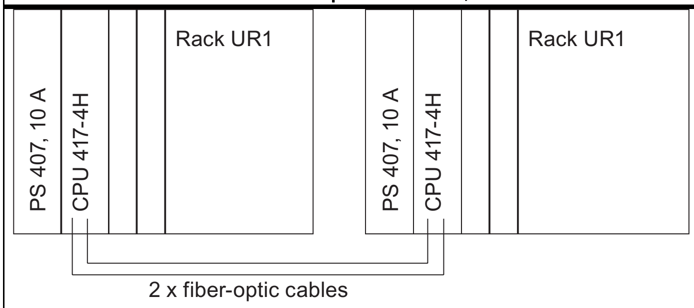
The following system containing one CPU (e.g. 417-4H) operating in stand-alone mode forms the basis for the calculation of a reference factor which defines the multiple of the availability of other systems with centralized I/Os compared to the base line.

Fault-tolerant CPU in stand-alone mode

Fault-tolerant CPU in stand-alone mode (e.g. 417-4H)	Factor
	1

Redundant CPUs in different racks

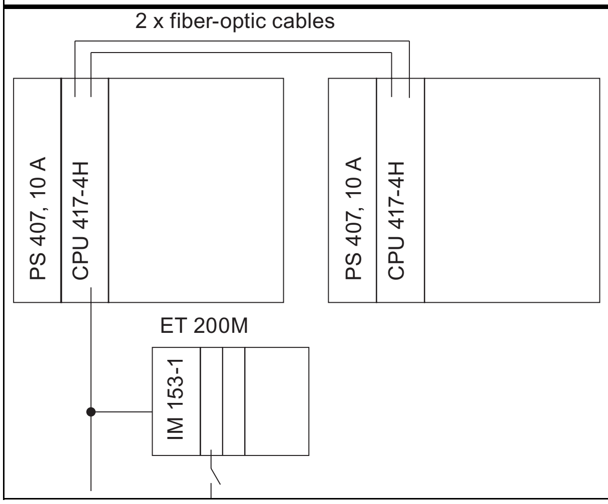
Redundant CPU 417-4H in a split rack, CCF = 2 %	Factor
	20

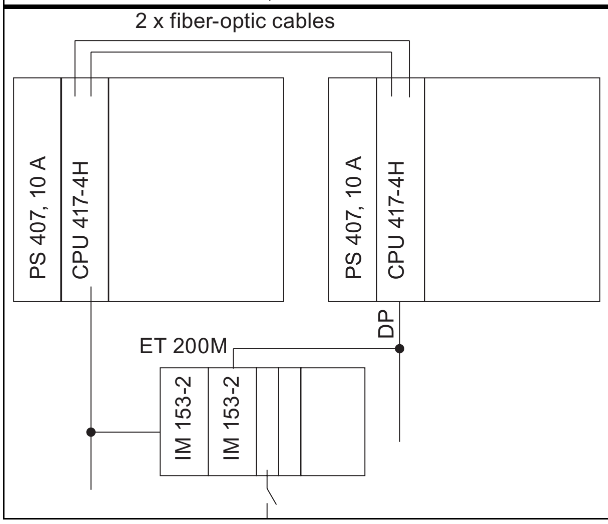
Redundant CPU 417-4H in separate racks, CCF = 1 %	Factor
	38

A.2.2 System configurations with distributed I/Os

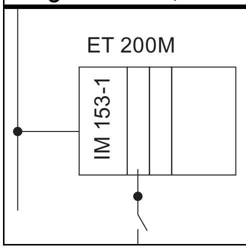
The system with two fault-tolerant CPUs 417-4 H and one-sided I/Os described below is taken as a basis for calculating a reference factor which specifies the multiple of the availability of the other systems with distributed I/Os compared with the base line.

Redundant CPUs with single-channel, one-sided or switched I/Os

<table>
<tr><th>One-sided distributed I/Os</th><th>Base line</th></tr>
<tr><td>
</td><td>1</td></tr>
</table>

<table>
<tr><th>Switched distributed I/O, CCF = 2 %</th><th>Factor</th></tr>
<tr><td>
</td><td>15</td></tr>
</table>

Redundant CPUs with redundant I/Os

Single-channel, one-sided I/O	MTBF factor
	1

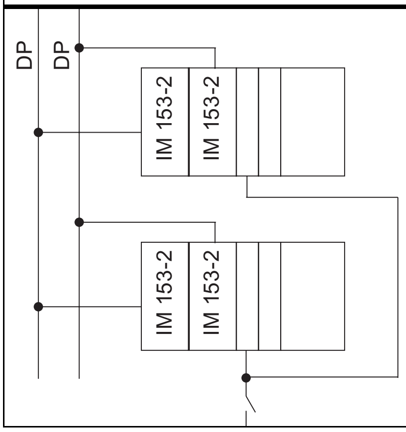
Redundant I/O	MTBF factor
	See following table

Table A–1 MTBF factors of the redundant I/Os

Module	Order number	MTBF factor CCF = 1 %	MTBF factor CCF = 0,2 %
Digital input modules, distributed			
DI 24xDC24V	6ES7326–1BK00–0AB0	100	500
DI 8xNAMUR [EEx ib]	6ES7326–1RF00–0AB0	100	500
DI16xDC24V, Alarm	6ES7321–7BH00–0AB0	4	4
Analog input modules, distributed			
AI 6x13-bit	6ES7336–1HE00–0AB0	100	500
AI8x12-bit	6ES7331–7KF02–0AB0	5	5
Digital output modules, distributed			
DO 10xDC24V/2A	6ES7326–2BF00–0AB0	100	500
DO8xDC24V/2A	6ES7322–1BF01–0AA0	3	4
DO32xDC24V/0.5A	6ES7322–1BL00–0AA0	3	4

Summary

There are now several thousand applications of redundant automation systems in the field, in various configurations. To calculate the MTBF, we assumed an average configuration.

Based on experience in the field, we may assume a total operating time of all redundant automation systems of 300,000,000 hours. We have received reports of the failure of four redundant automation systems in total.

This proves an assumed MTBF of 3000 years to be 95% reliable.

The MTBF values assessed as being real are:

Type I b, CCF = 2 % Approx. 230 years

Type I b, CCF = 0.2 % Approx. 1,200 years

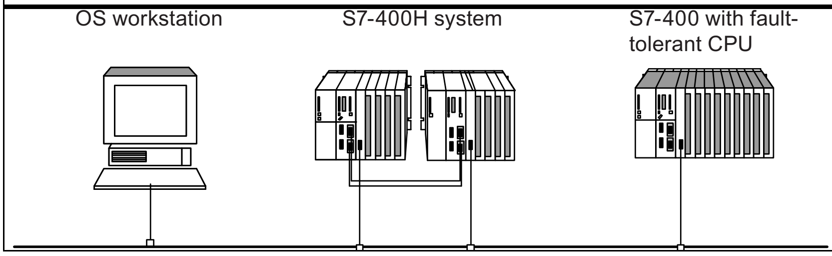
Type I differs from an average redundant automation system only in the use of a redundant power supply. So, the above analysis is rather pessimistic.

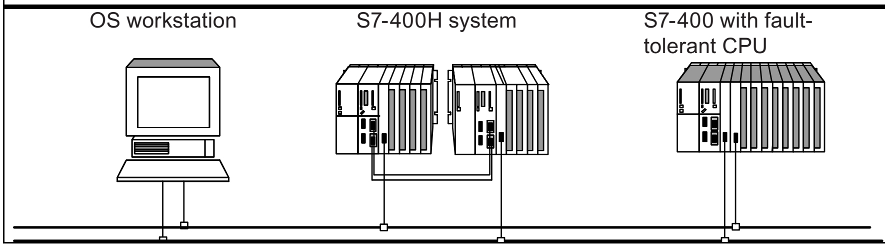
A.2.3 Comparison of system configurations with standard and fault-tolerant communication

The next section shows a comparison between standard and fault-tolerant communication for a configuration consisting of a fault-tolerant system, a fault-tolerant CPU operating in stand-alone mode, and a single-channel OS.

The comparison only took account of the CP and cable communication components.

Systems with standard and fault-tolerant communication

Standard communication	Base line
	1

Fault-tolerant communication	Factor
	approx. 80

B Stand-alone operation

Overview

This appendix provides the necessary information for you to operate a fault-tolerant CPU (414-4H or 417-4H) in stand-alone mode. You will learn:

- how stand-alone mode is defined
- when stand-alone mode is required
- what you have to take into account for stand-alone operation
- how the fault tolerance-specific LEDs react
- how to configure stand-alone operation of a fault-tolerant CPU
- how you can expand it to form a fault-tolerant system

The differences from a standard S7-400 CPU that you have to take into account when configuring and programming the fault-tolerant CPU are given in appendix Differences between fault-tolerant systems and standard systems (Page 369).

Definition

By stand-alone operation, we mean the use of a fault-tolerant CPU in a standard SIMATIC-400 station.

Reasons for stand-alone operation

The applications outlined below are only possible when using a fault-tolerant CPU, so are not operable with standard S7-400 CPUs.

- Use of fault-tolerant connections
- Configuration of the S7-400F fail-safe automation system

  A fail-safe user program can only be compiled for execution on a fault-tolerant CPU with a fail-safe F-Runtime license (for more details refer to the *S7-400F and S7-400FH Programmable Controllers* manuals).

  Note

  The self-test of the fault-tolerant CPU is also performed in stand-alone mode.

What you have to take into account for stand-alone operation of a fault-tolerant CPU

NOTICE
When operating a fault-tolerant CPU in stand-alone mode no synchronization modules may be connected. The rack number must be set to "0".

Although a fault-tolerant CPU has additional functions compared to a standard S7-400 CPU, it does not support specific functions. So particularly when programming your automation system, you need to know the CPU on which you are going to run the user program. A user program written for a standard S7-400 CPU usually will not run on a fault-tolerant CPU in stand-alone mode without adaptation.

The table below lists the differences between the operation of a fault-tolerant CPU in stand-alone mode and in redundant mode.

Table B-1 Differences between stand-alone mode and redundant mode

Function	Fault-tolerant CPU in stand-alone mode	Fault-tolerant CPU in redundant mode
Connection of S5 modules via IM or adapter casing	via IM 463–2	No
Redundancy error OBs (OB70, OB72)	Yes, but no calls	Yes
CPU hardware fault (OB 84)	after the detection and elimination of memory errors	after the detection and elimination of memory errors with reduced performance of the redundant link between the two CPUs
SSL ID W#16#0232 index W#16#0004 byte 0 of the "index" word in the data record	W#16#F8	Single mode: W#16#F8 or W#16#F9 Redundant: W#16#F8 and W#16#F1 or W#16#F9 and W#16#F0
Multi-DP master mode	Yes	No
System modifications in operation	Yes, as described in the "System Modification during Operation Using CIR" manual.	Yes, as described in chapter Failure and replacement of components during operation (Page 201) for redundant operation.

Fault tolerance-specific LEDs

The REDF, IFM1F, IFM2F, MSTR, RACK0 and RACK1 LEDs show the reaction specified in the table below in stand-alone mode.

LED	Reaction
REDF	Unlit
IFM1F	Unlit
IFM2F	Unlit
MSTR	Lit
RACK0	Lit
RACK1	Unlit

Configuring stand-alone mode

Requirement: No synchronization module may be inserted in the fault-tolerant CPU.

Procedure:

1. Insert a SIMATIC-400 station in your project.
2. Configure the station with the fault-tolerant CPU according to your hardware setup. For stand-alone operation, insert the fault-tolerant CPU in a standard rack (Insert > Station > S7–400 station in SIMATIC Manager).
3. Configure the parameters of the fault-tolerant CPU. Use the default values, or customize the necessary parameters.
4. Configure the necessary networks and connections. For stand-alone operation you can configure "fault-tolerant" S7 connections.

For help on procedure refer to the Help topics in SIMATIC Manager.

Expansion to a fault-tolerant system

⚠ WARNING
You can only expand your system to a fault-tolerant system if you have not assigned any odd numbers to expansion units in stand-alone mode.

To expand the fault-tolerant CPU later to form a fault-tolerant system:

1. Open a new project and insert a fault-tolerant station.
2. Copy the entire rack from the standard SIMATIC-400 station and insert it twice into the fault-tolerant station.
3. Insert the subnets as required.
4. Copy the DP slaves from the old stand-alone project to the fault-tolerant station as required.
5. Reconfigure the communication connections.
6. Carry out all changes required, such as the insertion of one-sided I/Os.

For information on how to configure the project refer to the Online Help.

Changing the operating mode of a fault-tolerant CPU

The procedure for changing the operating mode of a fault-tolerant CPU differs depending on the operating mode you want to switch to and rack number configured for the CPU:

Changing from redundant to stand-alone mode

1. Remove the synchronization modules
2. Remove the CPU.
3. Set rack number 0 on the CPU.
4. Install the CPU.
5. Download a project with the stand-alone configuration to the CPU.

Changing from stand-alone mode to redundant mode, rack number 0

1. Insert the synchronization modules into the CPU.
2. Run an unbuffered power cycle, for example by removing and inserting the CPU, or download a project to the CPU in which it is configured for redundant mode.

Changing from stand-alone mode to redundant mode, rack number 1

1. Set rack number 1 on the CPU.
2. Install the CPU.
3. Insert the synchronization modules into the CPU.

System modification during operation in stand-alone mode

With a system modification during operation, it is also possible to make certain configuration changes in RUN on fault-tolerant CPUs. The procedure corresponds to that for standard CPUs. Processing is halted during this, but for no more than 2.5 seconds (configurable), During this time, the process outputs retain their current values. In process control systems in particular, this has virtually no effect on the process. See also the *"Modifying the System during Operation via CiR"* manual.

System modifications during operation are only supported with distributed I/O. They require a configuration as shown in the figure below. To avoid overcomplicating the matter, this shows only one DP master system and one PA master system.

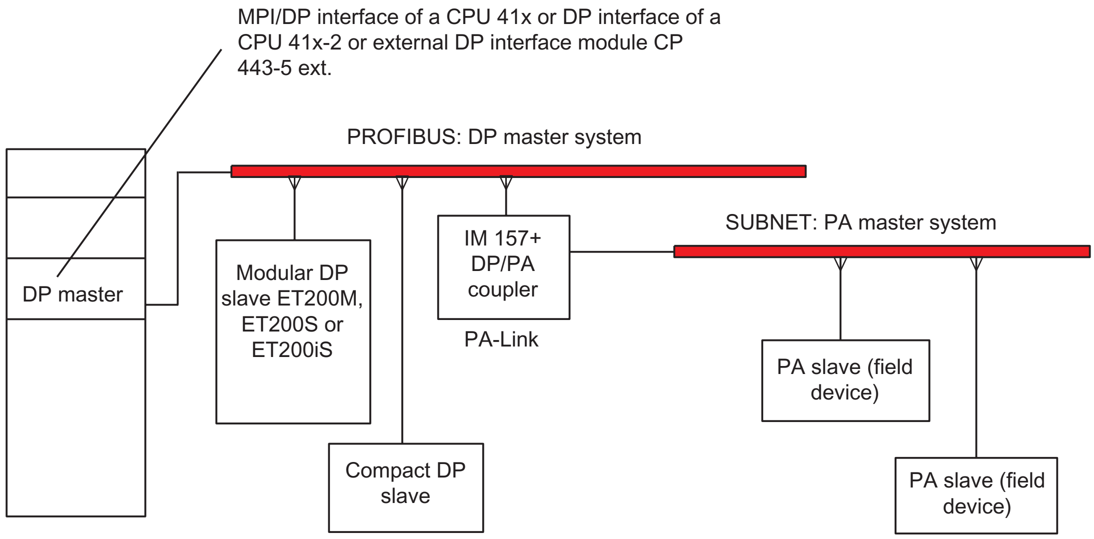


Figure B-1 Overview: System structure for system modifications during operation

Hardware requirements for system modifications during operation

To modify a system during operation, the following hardware requirements must be met at the commissioning stage:

- Use of an S7 400 CPU
- S7 400 H CPU only in stand-alone mode
- If you use a CP 443-5 Extended, this must have a firmware V5.0 or higher.
- To add modules to an ET 200M: Use an IM153-2, version MLFB 6ES7153-2BA00-0XB0 or higher, or an IM153-2FO, version MLFB 6ES7153-2BB00-0XB0 or higher. The installed ET 200M also requires an active backplane bus with sufficient free space for the planned expansion. Include the ET 200M so that it complies with IEC 61158.
- If you want to add entire stations: Make sure that you have the required connectors, repeaters, etc.
- If you want to add PA slaves (field devices): Use IM157 version MLFB 6ES7157-0AA82-0XA00 or higher in the corresponding DP/PA Link.

Note

You can freely combine components which support system modifications during operation with those that do not. Depending on your selected configuration, there may be restrictions affecting the components on which you can make system modifications during operation.

Software requirements for system modifications during operation

To make modifications during operation, the user program must be written so that station failures or module faults, for example, do not lead to a CPU STOP.

Permitted system modifications: Overview

During operation, you can make the following system modifications:

- Add components or modules with modular DP slaves ET 200M, ET 200S and ET 200iS, provided they are compliant with IEC 61158
- Use of previously unused channels in a module or submodule of the modular slaves ET 200M, ET 200S and ET 200iS
- Add DP slaves to an existing DP master system.
- Add PA slaves (field devices) to an existing PA master system
- Add DP/PA couplers downstream of an IM157
- Add PA Links (including PA master systems) to an existing DP master system.
- Assign added modules to a process image partition.
- Change parameter settings for I/O modules, for example selecting different interrupt limits.
- Undo changes: Modules, submodules, DP slaves and PA slaves (field devices) you added earlier can be removed again.

Migrating from S5-H to S7-400H C

This appendix will help you to migrate to fault-tolerant S7 systems if you are already familiar with the fault-tolerant systems of the S5 family.

Basic knowledge of the STEP7 configuration software is required for converting from the S5-H to the S7-400H.

C.1 General aspects

Documentation

The following manuals are available to familiarize you with the STEP 7 base software:

- *Configuring hardware and connections in STEP 7*
- *Programming with STEP 7*

Information on the various programming languages is available in the reference manuals listed below.

- *System and Standard Functions*
- STL, LAD, FBD for S7-300/400

The *From S5 to S7* manual supports you with details on migration.

C.2 Configuration, programming and diagnostics

Configuration

Configuration was performed in STEP 5 using a dedicated configuration package, such as COM 155H.

In STEP 7, the fault-tolerant CPUs are configured using the base software. In SIMATIC Manager, you can create a fault-tolerant station and configure it in HW CONFIG. The special features of the redundant CPUs are grouped on a small number of tabs. Integration into networks and configuration of connections is handled with NetPro.

Diagnostics and programming

In S5, error diagnostics are implemented with the help of the error data block to which the system writes all error data. Error OB 37 is started automatically when any entries are made. Further information has been stored in the H memory word.

The H memory word consists of a status byte and a control byte. Control information can be set in a bit pattern in the STEP 5 user program.

In STEP 7, system diagnostics is accomplished by means of the diagnostics buffer or by displaying what are known as partial lists from the system status list (specific information for fault-tolerant systems, for example, is located in SSL71). This query can be performed with the help of the PG or in the user program with SFC 51 "RDSYSST".

OB 70 is available for I/O redundancy loss, and OB 72 for CPU redundancy loss.

The function of the control byte is implemented in STEP 7 by means of SFC 90 "H_CTRL".

Topic in S5	Equivalent in S7
Error OB37	Error OBs OB 70 and OB 72
Memory control word	SFC 90 "H_CTRL"
Memory status word	SSL71
Error block	Diagnostics buffer

D Differences between fault-tolerant systems and standard systems

When configuring and programming a fault-tolerant automation system with fault-tolerant CPUs, you must make allowances for a number of differences from the standard S7-400 CPUs. Although a fault-tolerant CPU has additional functions compared to a standard S7-400 CPU, it does not support specific functions. This has to be taken in account particularly if you wish to run a program that was created for a standard S7-400 CPU on a fault-tolerant CPU.

The ways in which the programming of fault-tolerant systems differs from that for standard systems are summarized below. You will find further differences in appendix Stand-alone operation (Page 361).

If you use any of the affected calls (OBs and SFCs) in your user program, you will need to adapt your program accordingly.

Additional functions of fault-tolerant systems

Function	Additional programming
Redundancy error OBs	• I/O redundancy error OB (OB 70) • CPU redundancy error OB (OB 72) For detailed information, refer to the *System and Standard Functions* reference manual.
CPU hardware fault	OB 84 is also called if the performance of the redundant link between the two CPUs is reduced.
Additional information in OB start information and in diagnostics buffer entries	The rack number and the CPU (master/standby) are specified. You can evaluate this additional information in the program.
SFC for fault-tolerant systems	You can control processes in fault-tolerant systems using SFC 90 "H_CTRL".
Fault-tolerant communication connections	Fault-tolerant connections are configured and do not require further programming. You can use the SFBs for configured connections when using fault-tolerant connections.
Self-test	The self-test is performed automatically, no further programming is required,
High-quality RAM test	The CPU performs a high-quality RAM test after an unbuffered POWER ON.
Switched I/O	No additional programming required, see section Using single-channel switched I/Os (Page 133).

Function	Additional programming
Information in the system status list	• You can also obtain data records for the fault tolerance-specific LEDs from the partial list using the SSL ID W#16#0019. • You can also obtain data records for the redundancy error OBs from the partial list using the SSL ID W#16#0222. • You can obtain information on the current status of the fault-tolerant system using the partial list with SSL ID W#16#xy71. • You can also obtain data records for the fault tolerance-specific LEDs from the partial list using the SSL ID W#16#0174. • The partial list with the SSL-ID W#16#xy75 provides information on the status of the communication between the fault-tolerant system and switched DP slaves.
Update monitoring	The operating system monitors the following four configurable timers: • Maximum cycle time extension • Maximum communication delay • Maximum inhibit time for priority classes > 15 • Minimum I/O retention time No additional programming is required for this. For more detailed information, refer to chapter Link-up and update (Page 99).
SSL ID W#16#0232 index W#16#0004 byte 0 of the "index" word in the data record	Fault-tolerant CPU in stand-alone mode: W#16#F8 Fault-tolerant CPU in solo mode: W#16#F8 or W#16#F9 Fault-tolerant CPU in redundant mode: W#16#F8 and W#16#F1 or W#16#F9 and W#16#F0

Restrictions of the fault-tolerant CPU compared to a standard CPU

Function	Restriction of the fault-tolerant CPU
Warm restart	A hot restart is not possible. OB 101 is not possible
Multicomputing	Multicomputing is not possible. OB 60 and SFC 35 are not supported
Startup without configuration loaded	Startup without loaded configuration is not possible.
Background OB	OB 90 is not supported.
Multi-DP master mode	The fault-tolerant CPUs do not support multi-DP master mode in REDUNDANT mode.
Direct communication between DP slaves	Can not be configured in STEP 7
Equidistance for DP slaves	No equidistance for DP slaves in the fault-tolerant system
Synchronization of DP slaves	Synchronization of DP slave groups is not supported. SFC 11 "DPSYC_FR" is not supported.
Disabling and enabling DP slaves	Disabling and enabling DP slaves is not possible. SFC 12 "D_ACT_DP" is not supported.
Insertion of DP modules in the module slots for interface modules	Not possible. The module slots are designed only for use by synchronization modules.

Function	Restriction of the fault-tolerant CPU
Runtime response	The command execution time for a CPU 41x–4H is slightly higher than for a corresponding standard CPU (see *S7–400 Instruction List* and *S7-400H Instruction List*). This must be taken into account for all time-critical applications. You may need to increase the cycle monitoring time.
DP cycle time	A CPU 41x-4H has a slightly longer DP cycle time than the corresponding standard CPU.
Delays and inhibits	During update: • The asynchronous SFCs for data records are acknowledged negatively • Messages are delayed • All priority classes up to 15 are initially delayed • Communication requests are rejected or delayed • Finally, all priority classes are disabled For more detailed information, refer to chapter 7.
Use of symbol-oriented messages (SCAN)	The use of symbol-oriented messages is not possible.
Global data communication	GD communication is not possible (neither cyclically, nor by calling system functions SFC 60 "GD_SND" and SFC 61 "GD_RCV")
S7 basic communication	Communication functions (SFCs) for basic communication are not supported.
Open block communication	Open block communication is not supported by the S7-400H.
S5 connection	The connection of S5 modules by means of adapter casing is not possible. The connection of S5 modules via IM 463-2 is only supported in stand-alone mode.
CPU as DP slave	Not possible
Use of SFC49 "LGC_GADR"	You are operating an S7-400H automation system in redundant mode. If you declare the logical address of module of the switched DP slave at the LADDR parameter and call SFC49, the high byte of the RACK parameter returns the DP master system ID of the active channel. If there is no active channel, the function outputs the ID of the DP master system belonging to the master CPU.
Call of SFC51 "RDSYSST" with SSL_ID=W#16#xy91	The data records of the SSL partial lists shown below can not be read with SFC51 "RDSYSST": • SSL_ID=W#16#0091 • SSL_ID=W#16#0191 • SSL_ID=W#16#0291 • SSL_ID=W#16#0391 • SSL_ID=W#16#0991 • SZL_ID=W#16#0E91
SFC 70/71 call	Not possible
Reading our the serial number of the memory card	Not possible
Resetting the CPU to the factory state	Not possible
Data record routing	Not possible

See also

System and operating states of the S7–400H (Page 83)

Function modules and communication processors supported by the S7-400H

E

You can use the following function modules (FMs) and communication processors (CPs) on an S7-400 automation system:

FMs and CPs usable centrally

Module	Order no.	Release	one-sided	Redundant
Counter module FM 450	6ES7450–1AP00–0AE0	Product release 2 or later	Yes	No
Function module FM 458-1 DP	6DD 1607-0AA1	As of firmware 1.1.0	Yes	Yes
Communications processor CP 441-1 (point-to-point link)	6ES7441–1AA02–0AE0	Product release 2 or later	Yes	No
	6ES7441–1AA03–0XE0	Product release 1 or later with firmware V1.0.0		
Communications processor CP 441-2 (point-to-point link)	6ES7441–2AA02–0AE0	Product release 2 or later	Yes	No
	6ES7441–2AA03–0XE0	Product release 1 or later with firmware V1.0.0		
Communications processor CP 443-1 Multi (Industrial Ethernet, TCP / ISO transport)	6GK7 443–1EX10–0XE0	Product version 1 or higher with firmware V2.6.7	Yes	Yes
	6GK7 443–1EX11–0XE0	Product version 1 or higher with firmware V2.6.7	Yes	Yes
Communication module CP 443-1 Multi (Industrial Ethernet ISO and TCP/IP 2-port switch)	6GK7 443–1EX20–0XE0	Product version 1 or later with firmware V1.0.26	Yes	Yes
Communications module CP 443-5 Basic (PROFIBUS; S7 communication)	6GK7 443–5FX01–0XE0	Product release 1 or later with firmware V3.1	Yes	Yes
Communications module CP 443-5 Extended (PROFIBUS; master on PROFIBUS DP) [1]	6GK7 443–5DX02–0XE0	Product release 2 or later with firmware V3.2.3	Yes	Yes
Communications module CP 443-5 Extended (PROFIBUS DPV1) [1] [2]	6GK7 443–5DX03–0XE0	Product version 2 or higher with firmware V5.1.0	Yes	Yes
Communications module CP 443-5 Extended (PROFIBUS DPV1) [1] [2]	6GK7 443–5DX04–0XE0	Product version 1 or higher with firmware V6.0	Yes	Yes

1) Only these modules should be used as external master interfaces on the PROFIBUS DP.

2) These modules support DPV1 as external DP master interface module (complying with IEC 61158/ EN 50170).

FMs and CPs usable for distributed one-sided use

Note

You can use all the FMs and CPs released for the ET 200M with the S7-400H in distributed and one-sided mode.

FMs and CPs usable for distributed switched use

Module	Order no.	Release
Communication processor CP 341–1 (point-to-point link)	6ES7341–1AH00–0AE0 6ES7341–1BH00–0AE0 6ES7341–1CH00–0AE0	Product release 3 or later
	6ES7341–1AH01–0AE0 6ES7341–1BH01–0AE0 6ES7341–1CH01–0AE0	Product release 1 or later with firmware V1.0.0
Communication processor CP 342–2 (ASI bus interface module)	6GK7 342–2AH01–0XA0	Product release 1 or later with firmware V1.10
Communication processor CP 343–2 (ASI bus interface module)	6GK7 343–2AH00–0XA0	Product release 2 or later with firmware V2.03
Counter module FM 350–1	6ES7350–1AH01–0AE0 6ES7350–1AH02–0AE0	Product release 1 or later
Counter module FM 350–2	6ES7350–2AH00–0AE0	Product release 2 or later
Controller module FM 355 C	6ES7355–0VH10–0AE0	Product release 4 or later
Controller module FM 355 S	6ES7355–1VH10–0AE0	Product release 3 or later
High-speed boolean processor FM 352-5	6ES7352–5AH00–0AE0	Product release 1 or later with firmware V1.0.0
Controller module FM 355-2 C	6ES7355–0CH00–0AE0	Product release 1 or later with firmware V1.0.0
Controller module FM 355-2 S	6ES7355–0SH00–0AE0	Product release 1 or later with firmware V1.0.0

NOTICE

One-sided or switched function and communication modules are **not** synchronized in the fault-tolerant system if they are in pairs, e.g. two identical FM 450 modules operating in one-sided mode do **not** synchronize their counter states.

Connection examples for redundant I/Os

F

F.1 SM 321; DI 16 x DC 24 V, 6ES7321–1BH02–0AA0

The diagram below shows the connection of two redundant encoders to two SM 321; DI 16 x DC 24 V. The encoders are connected to channel 0.

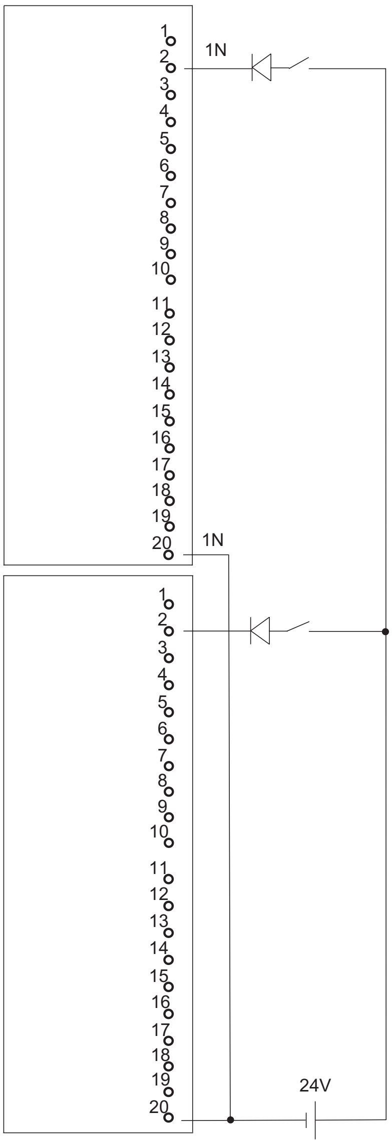


Figure F-1 Example of an interconnection with SM 321; DI 16 x DC 24 V

F.2 SM 321; DI 32 x DC 24 V, 6ES7321–1BL00–0AA0

The diagram below shows the connection of two redundant encoder pairs to two redundant SM 32; DI 32 x DC 24 V. The encoders are connected to channel 0 and channel 16 respectively.

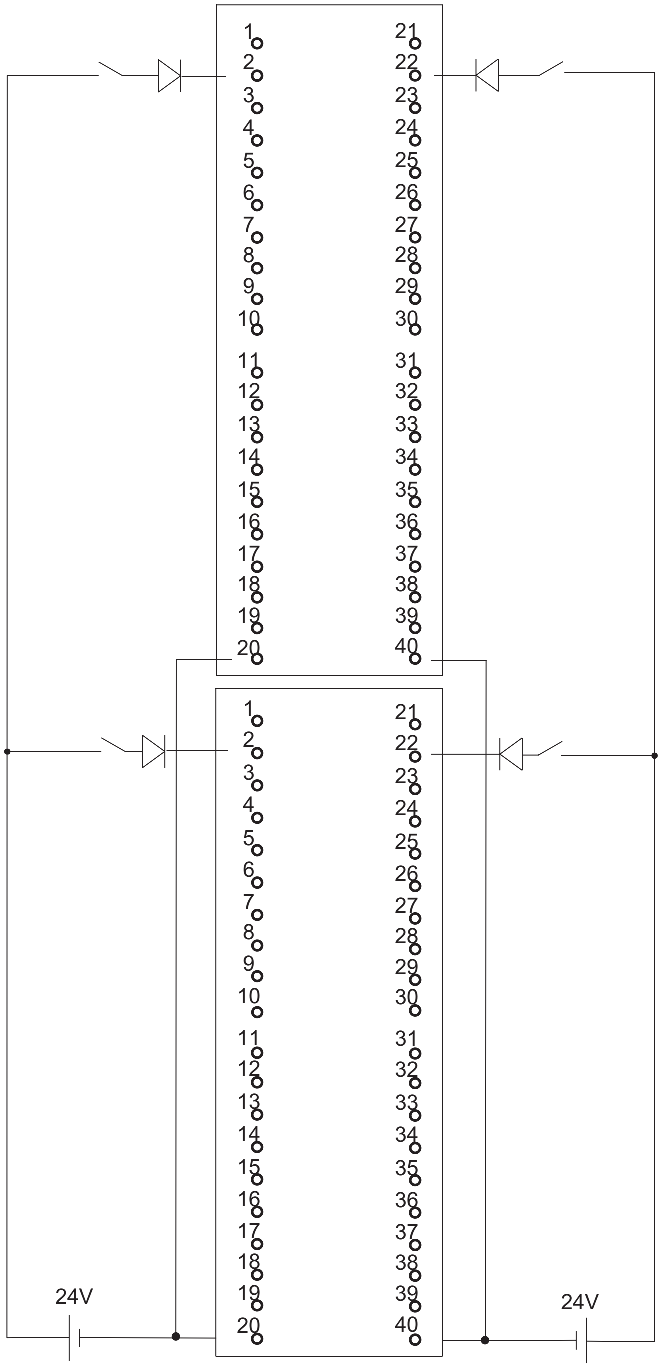


Figure F-2 Example of an interconnection with SM 321; DI 32 x DC 24 V

F.3 SM 321; DI 16 x AC 120/230V, 6ES7321–1FH00–0AA0

The diagram below shows the connection of two redundant encoders to two SM 321; DI 16 x AC 120/230 V. The encoders are connected to channel 0.

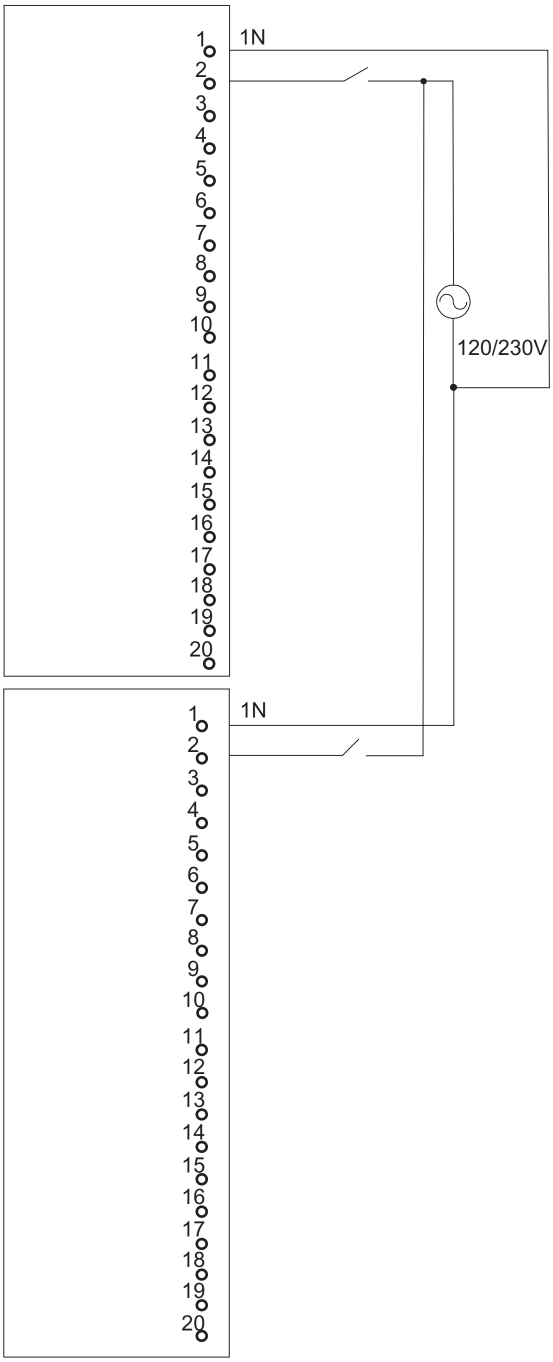


Figure F-3 Example of an interconnection with SM 321; DI 16 x AC 120/230 V

F.4 SM 321; DI 8 x AC 120/230 V, 6ES7321–1FF01–0AA0

The diagram below shows the connection of two redundant encoders to two SM 321; DI 8 AC 120/230 V. The encoders are connected to channel 0.

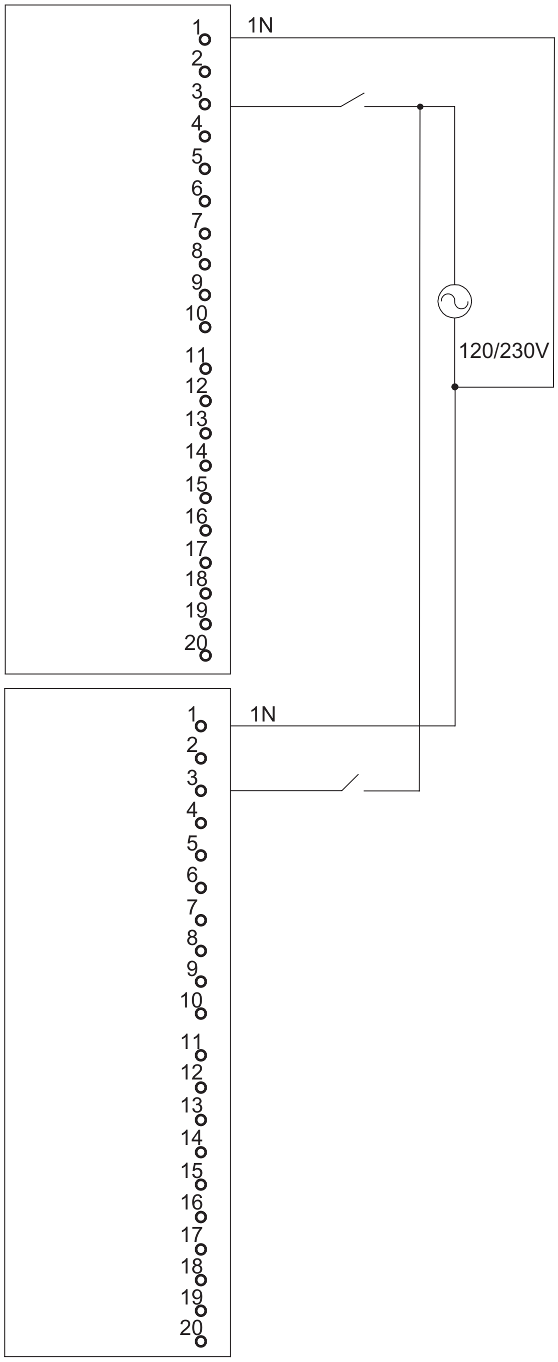


Figure F-4 Example of an interconnection with SM 321; DI 8 x AC 120/230 V

F.5 SM 321; DI 16 x DC 24V, 6ES7321–7BH00–0AB0

The diagram below shows the connection of two redundant encoder pairs to two SM 321; DI 16 x DC 24V. The encoders are connected to channels 0 and 8.

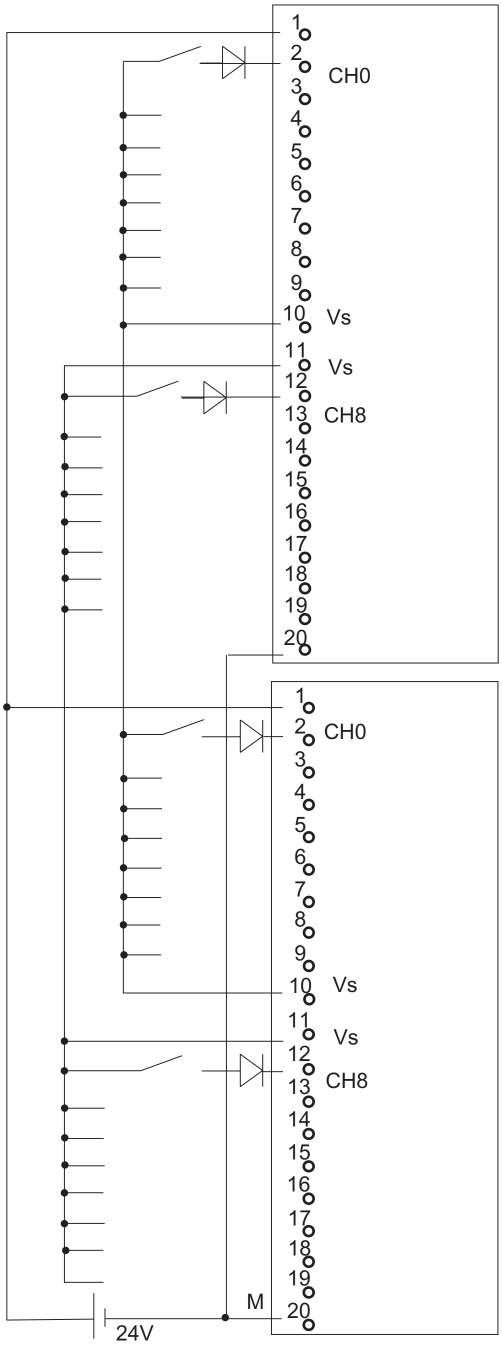


Figure F-5 Example of an interconnection with SM 321; DI 16 x DC 24V

F.6 SM 321; DI 16 x DC 24V, 6ES7321–7BH01–0AB0

The diagram below shows the connection of two redundant encoder pairs to two SM 321; DI 16 x DC 24V. The encoders are connected to channels 0 and 8.

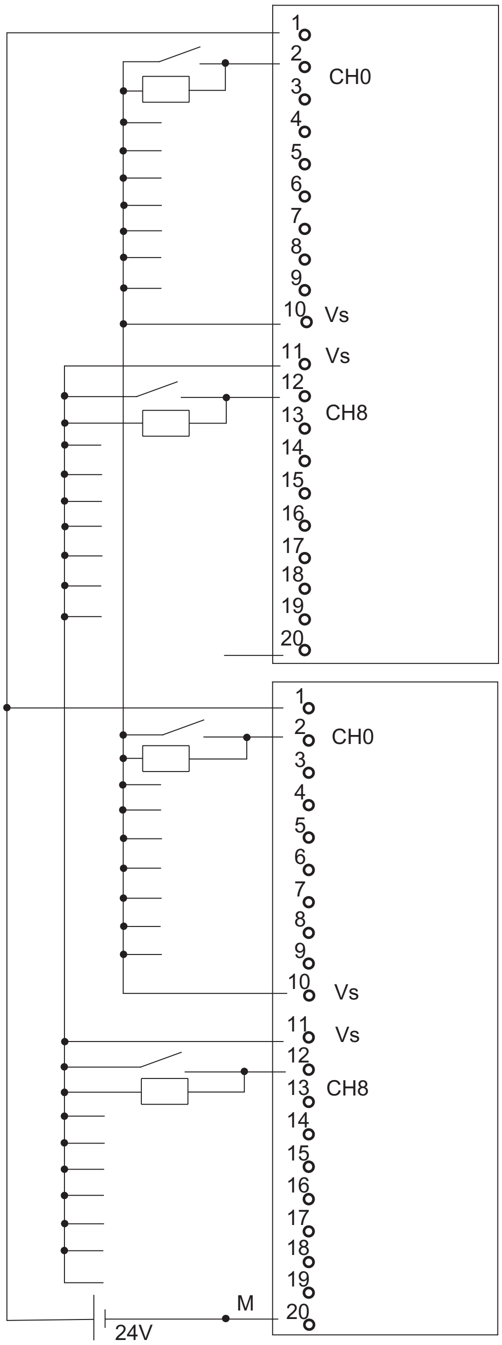


Figure F-6 Example of an interconnection with SM 321; DI 16 x DC 24V

F.7 SM 326; DO 10 x DC 24V/2A, 6ES7326–2BF01–0AB0

The diagram below shows the connection of an actuator to two redundant SM 326; DO 10 x DC 24V/2AV. The actuator is connected to channel 1.

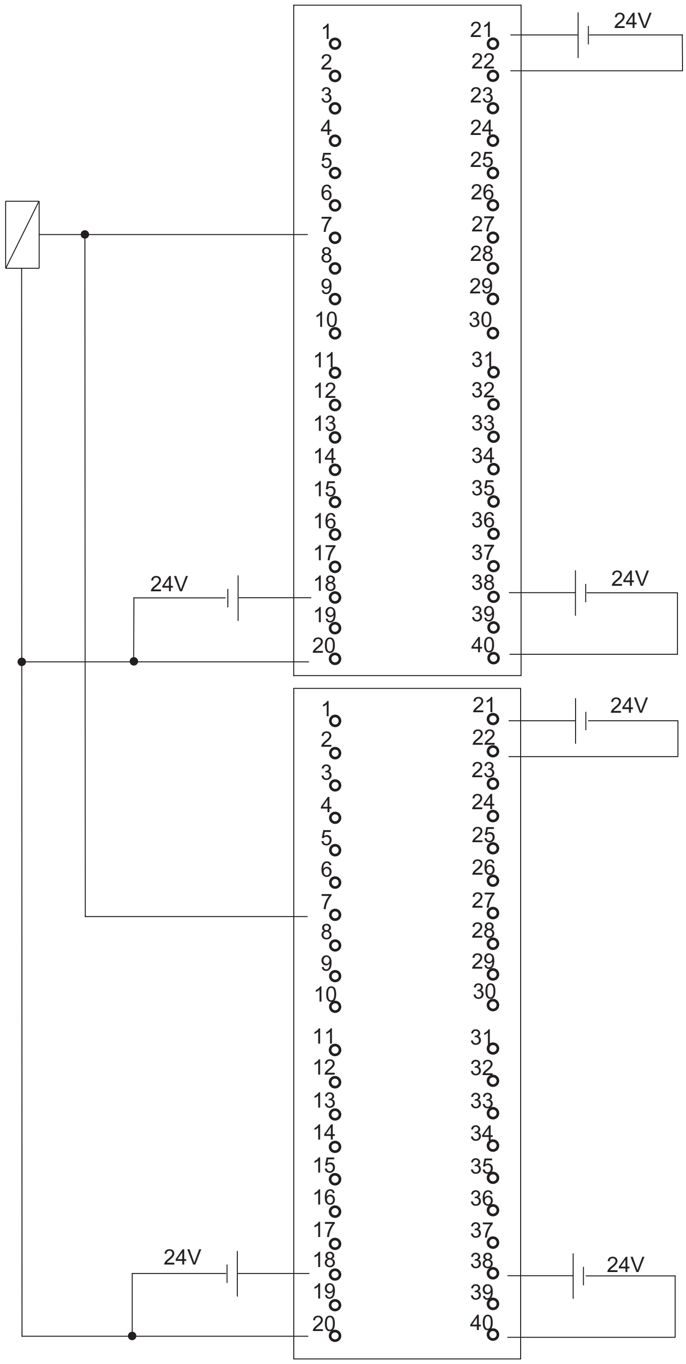


Figure F-7 Example of an interconnection with SM 326; DO 10 x DC 24 V/2 A

F.8 SM 326; DI 8 x NAMUR, 6ES7326–1RF00–0AB0

The diagram below shows the connection of two redundant encoders to two redundant SM 326; DI 8 x NAMUR. The encoders are connected to channel 13.

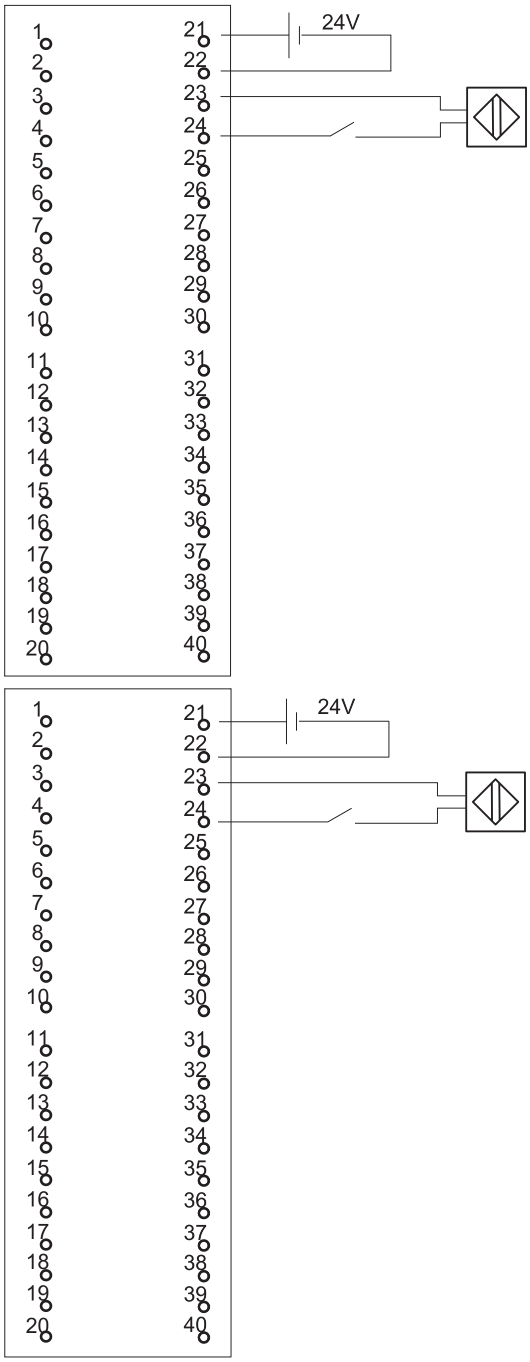


Figure F-8 Example of an interconnection with SM 326; DI 8 x NAMUR

F.9 SM 326; DI 24 x DC 24 V, 6ES7326–1BK00–0AB0

The diagram below shows the connection of one encoder to two redundant SM 326; DI 24 x DC 24 V. The encoder is connected to channel 13.

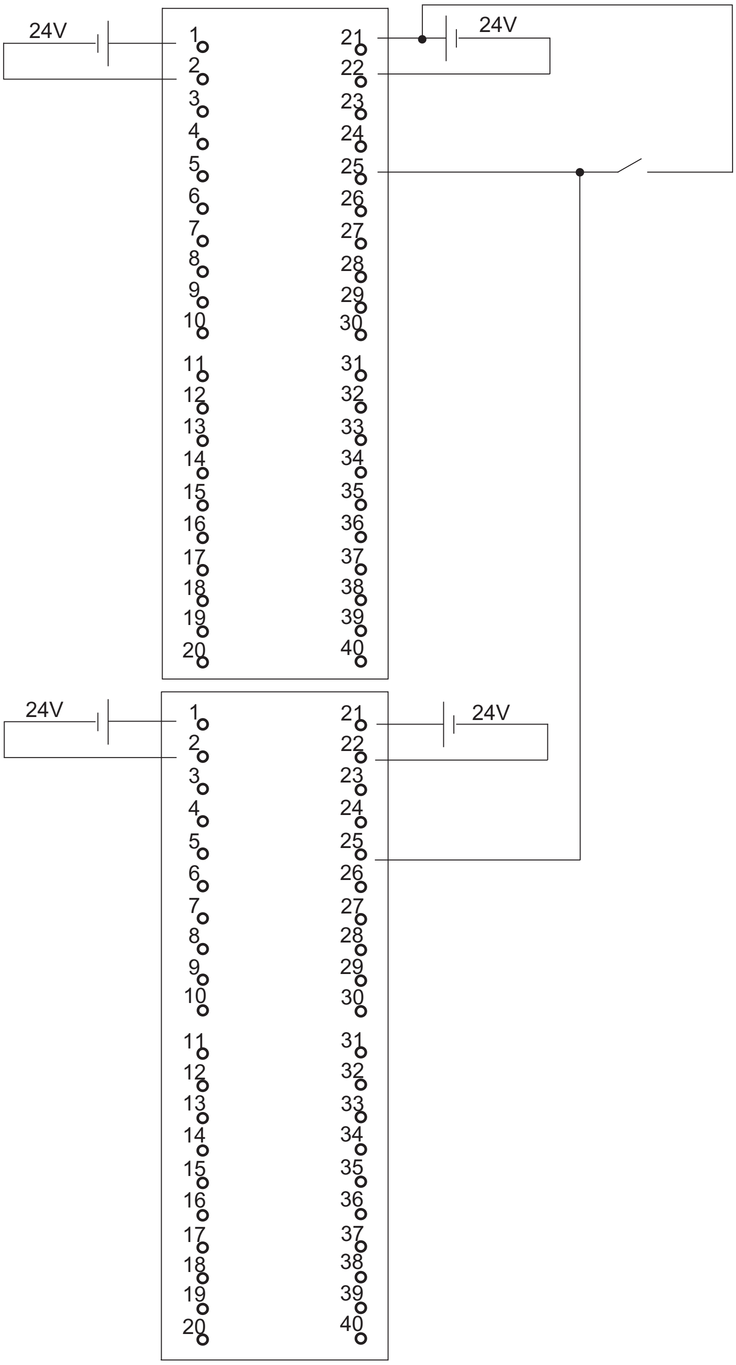


Figure F-9 Example of an interconnection with SM 326; DI 24 x DC 24 V

F.10 SM 421; DI 32 x UC 120 V, 6ES7421–1EL00–0AA0

The diagram below shows the connection of a redundant encoder to two SM 421; DI 32 x UC 120 V. The encoder is connected to channel 0.

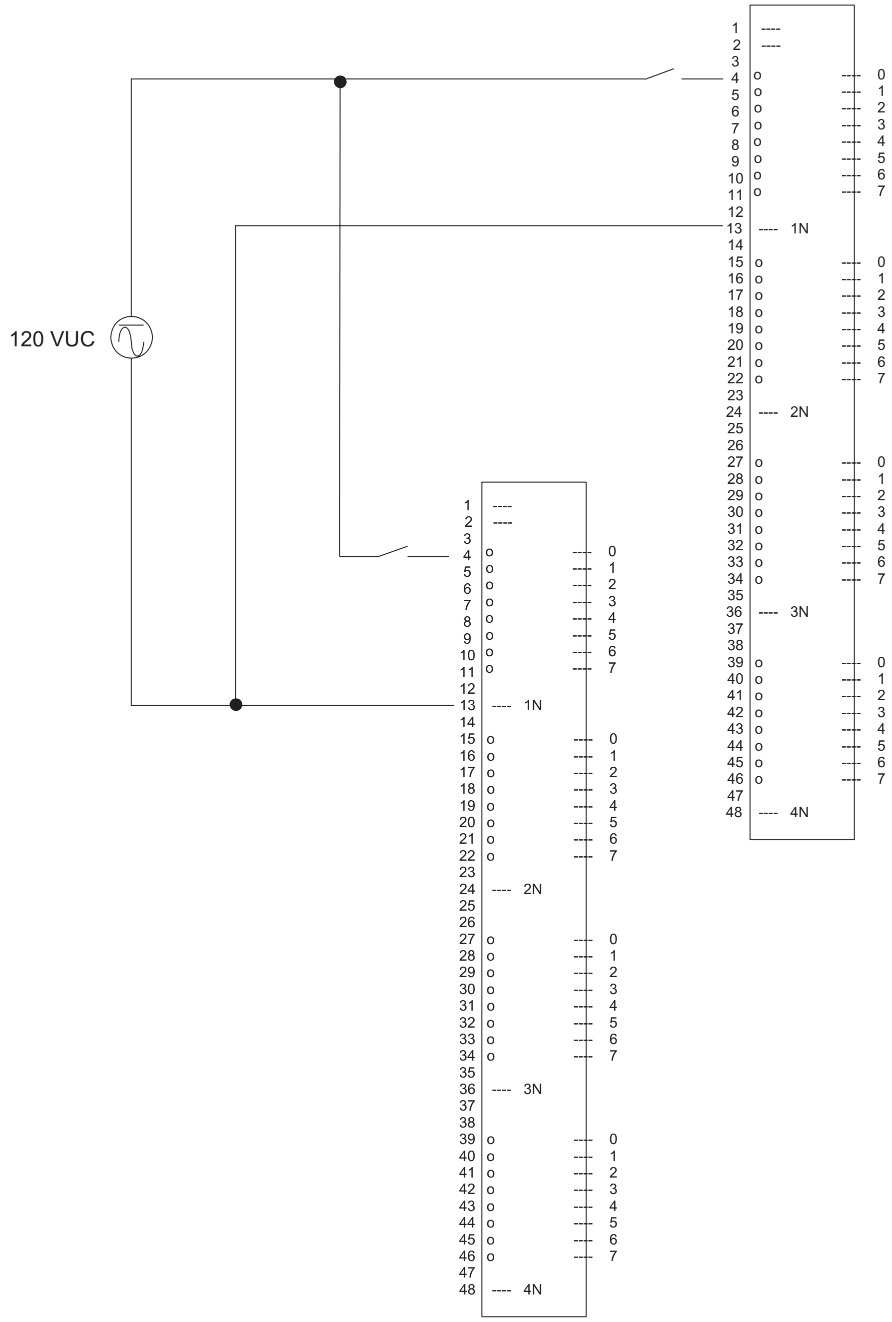


Figure F-10 Example of an interconnection with SM 421; DI 32 x UC 120 V

F.11 SM 421; DI 16 x DC 24 V, 6ES7421–7BH01–0AB0

The diagram below shows the connection of two redundant encoders pairs to two SM 421; D1 16 x 24 V. The encoders are connected to channel 0 and 8.

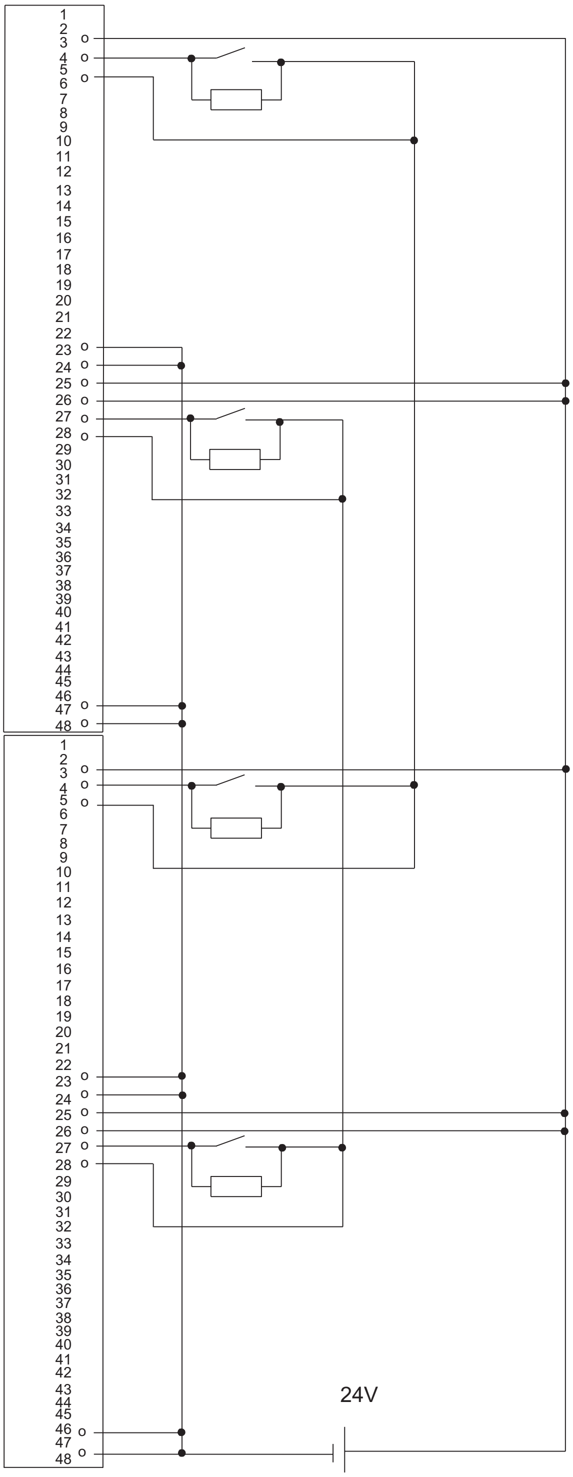


Figure F-11 Example of an interconnection with SM 421; DI 16 x 24 V

F.12 SM 421; DI 32 x DC 24 V, 6ES7421–1BL00–0AB0

The diagram below shows the connection of two redundant encoders to two SM 421; D1 32 x 24 V. The encoders are connected to channel 0.

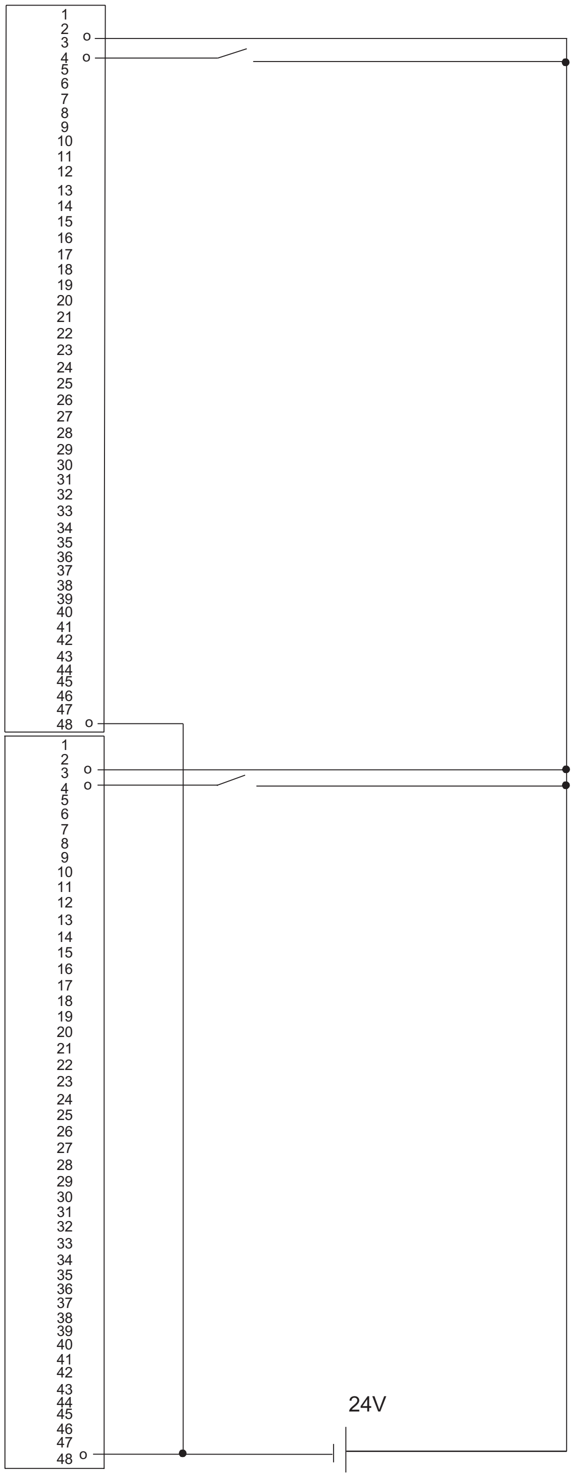


Figure F-12 Example of an interconnection with SM 421; DI 32 x 24 V

F.13 SM 421; DI 32 x DC 24 V, 6ES7421–1BL01–0AB0

The diagram below shows the connection of two redundant encoders to two SM 421; D1 32 x 24 V. The encoders are connected to channel 0.

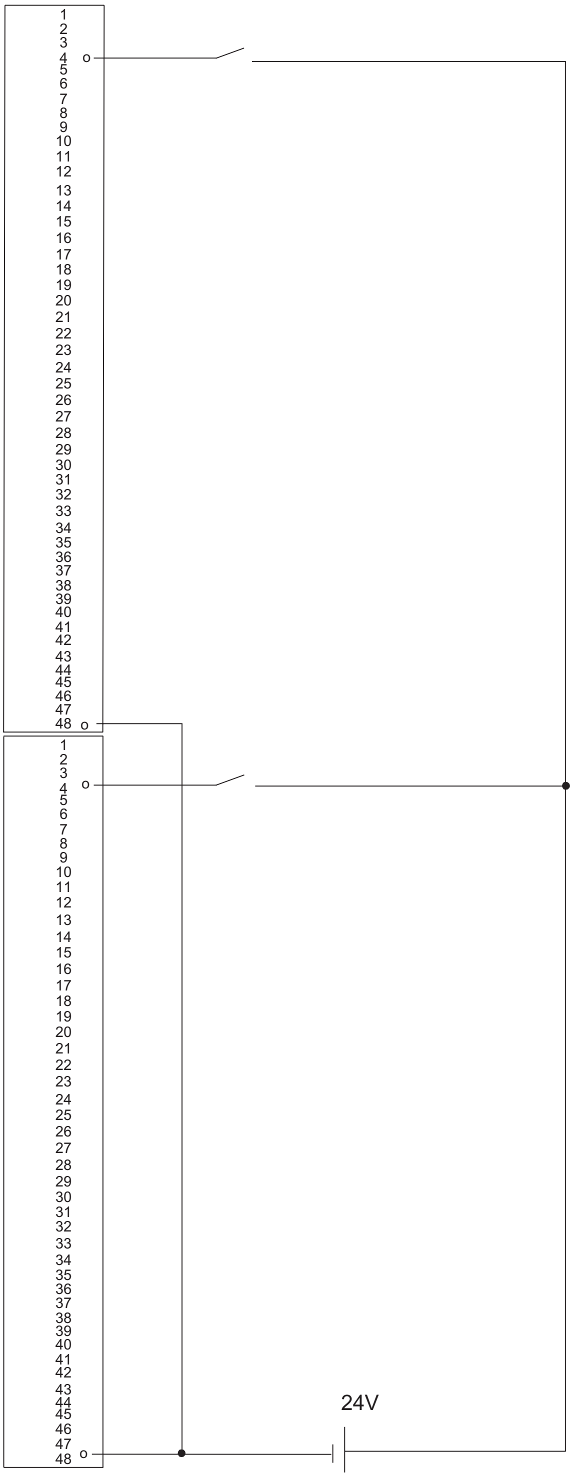


Figure F-13 Example of an interconnection with SM 421; DI 32 x 24 V

F.14 SM 322; DO 8 x DC 24 V/2 A, 6ES7322–1BF01–0AA0

The diagram below shows the connection of an actuator to two redundant SM 322; DO 8 x DC 24 V. The actuator is connected to channel 0.

Types with $U_{\_r}$ >=200 V and $I_{\_F}$ >= 2 A are suitable as diodes

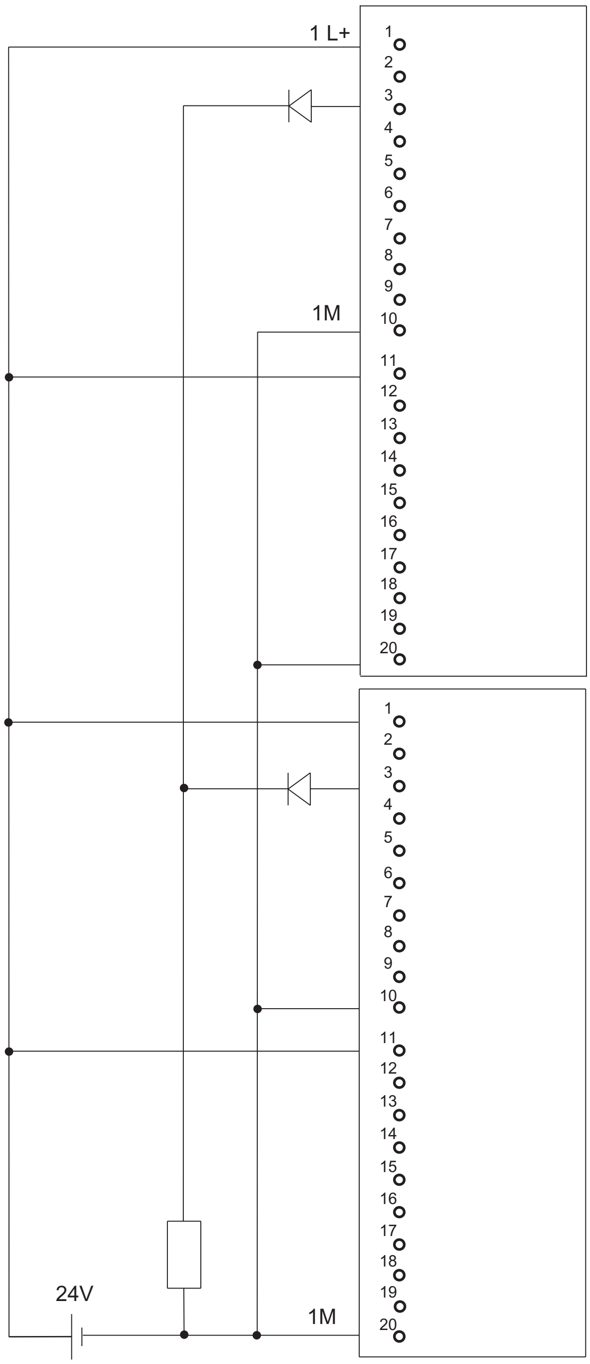


Figure F-14 Example of an interconnection with SM 322; DO 8 x DC 24 V/2 A

F.15 SM 322; DO 32 x DC 24 V/0,5 A, 6ES7322–1BL00–0AA0

The diagram below shows the connection of an actuator to two redundant SM 322; DO 32 x DC 24 V. The actuator is connected to channel 1.

Suitable diodes include types of the series 1N4003 ... 1N4007, or any other diode with U_r >=200 V and I_F >= 1 A

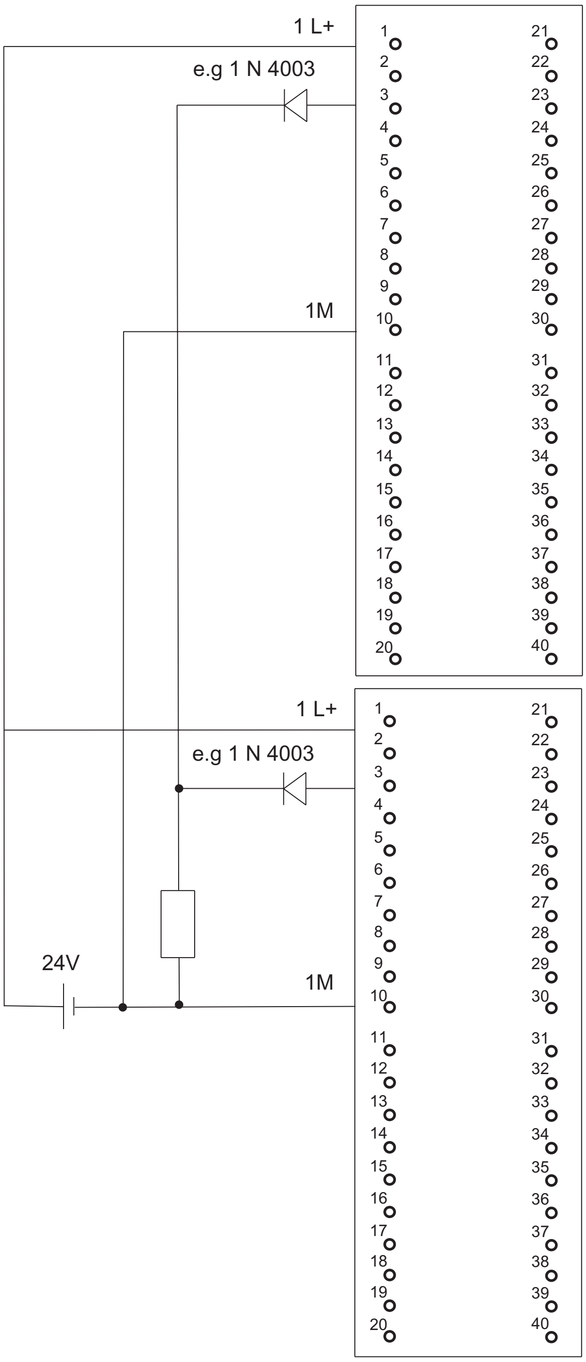


Figure F-15 Example of an interconnection with SM 322; DO 32 x DC 24 V/0.5 A

F.16 SM 322; DO 8 x AC 230 V/2 A, 6ES7322–1FF01–0AA0

The diagram below shows the connection of an actuator to two SM 322; DO 8 x AC 230V/2AV. The actuator is connected to channel 0.

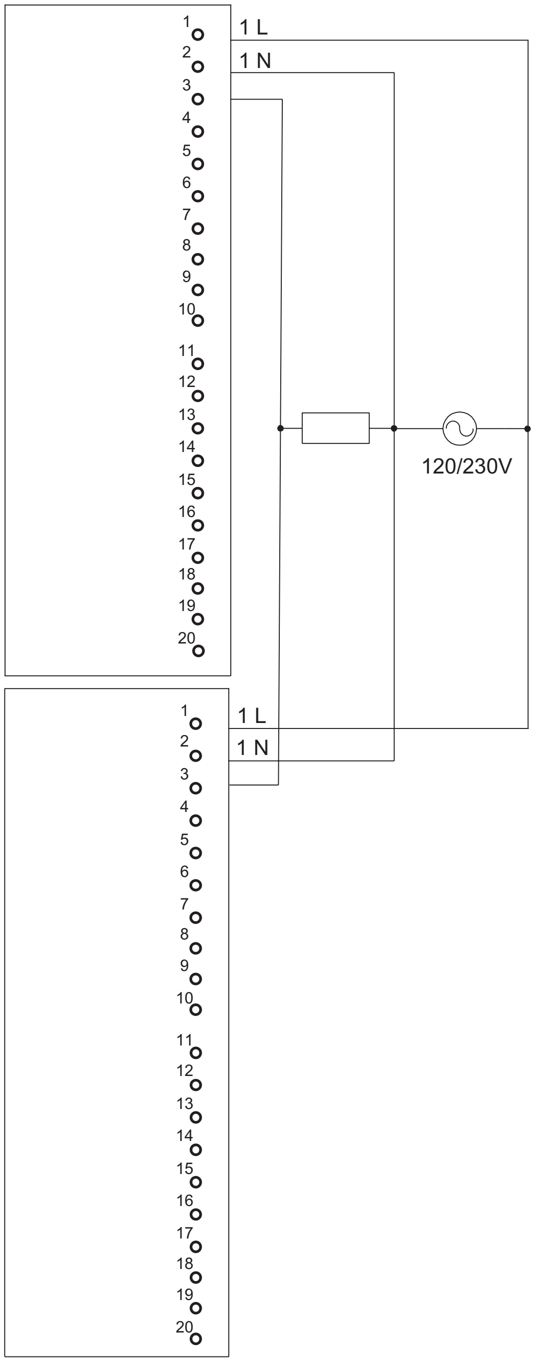


Figure F-16 Example of an interconnection with SM 322; DO 8 x AC 230 V/2 A

F.17 SM 322; DO 4 x DC 24 V/10 mA [EEx ib], 6ES7322–5SD00–0AB0

The diagram below shows the connection of an actuator to two SM 322; DO 16 x DC 24 V/10 mA [EEx ib]. The actuator is connected to channel 0. Suitable diodes include types of the series 1N4003 ... 1N4007, or any other diode with U_r >=200 V and I_F >= 1 A

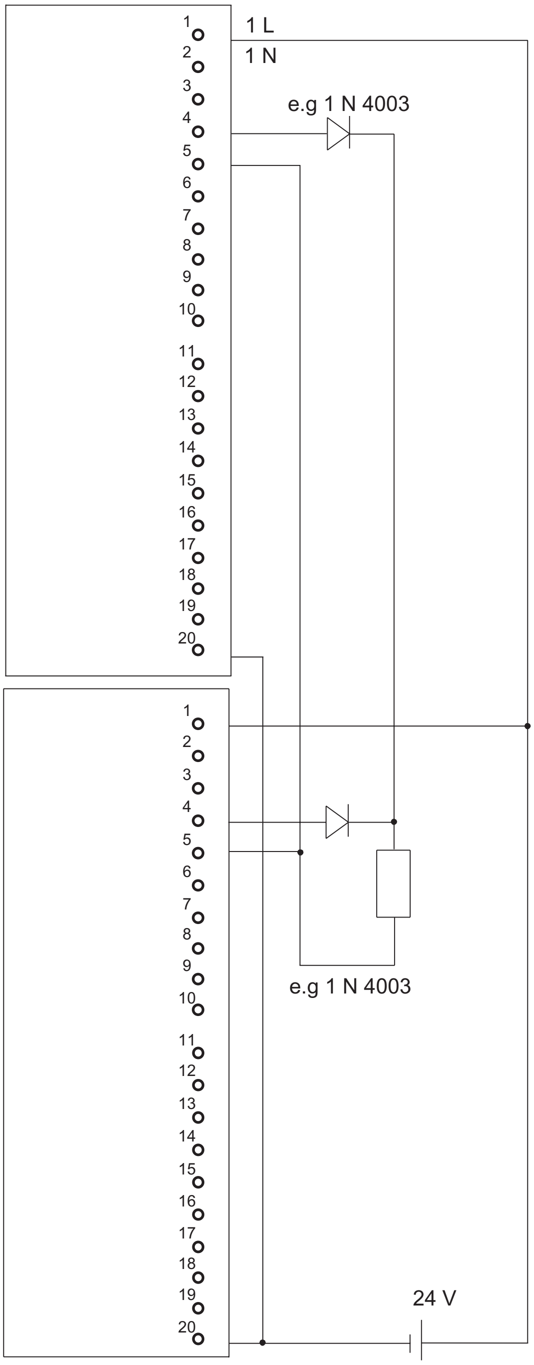


Figure F-17 Example of an interconnection with SM 322; DO 16 x DC 24 V/10 mA [EEx ib]

F.18 SM 322; DO 4 x DC 15 V/20 mA [EEx ib], 6ES7322–5RD00–0AB0

The diagram below shows the connection of an actuator to two SM 322; DO 16 x DC 15 V/20 mA [EEx ib]. The actuator is connected to channel 0. Suitable diodes are, for example, those of the series 1N4003 ... 1N4007, or any other diode with U_r >=200 V and I_F >= 1 A

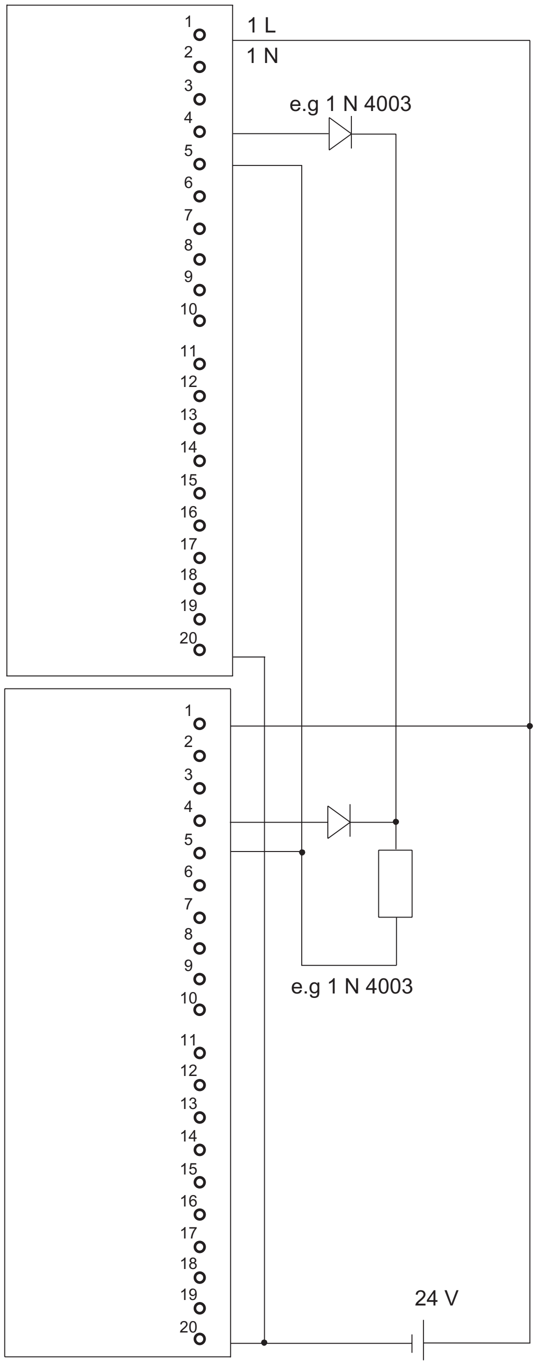


Figure F-18 Example of an interconnection with SM 322; DO 16 x DC 15 V/20 mA [EEx ib]

F.19 SM 322; DO 8 x DC 24 V/0,5 A, 6ES7322–8BF00–0AB0

The diagram below shows the connection of an actuator to two redundant SM 322; DO 8 x DC 24 V/0.5 A. The actuator is connected to channel 0.

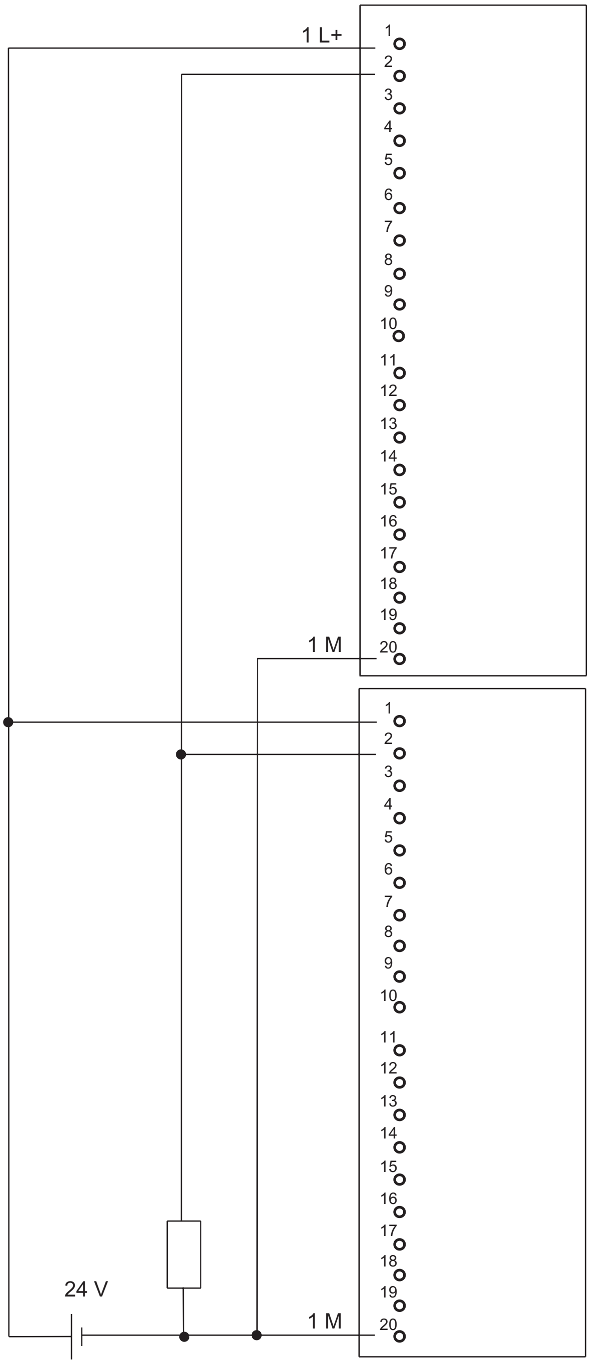


Figure F-19 Example of an interconnection with SM 322; DO 8 x DC 24 V/0.5 A

F.20 SM 322; DO 16 x DC 24 V/0,5 A, 6ES7322–8BH01–0AB0

The diagram below shows the connection of an actuator to two redundant SM 322; DO 16 x DC 24 V/0.5 A. The actuator is connected to channel 8.

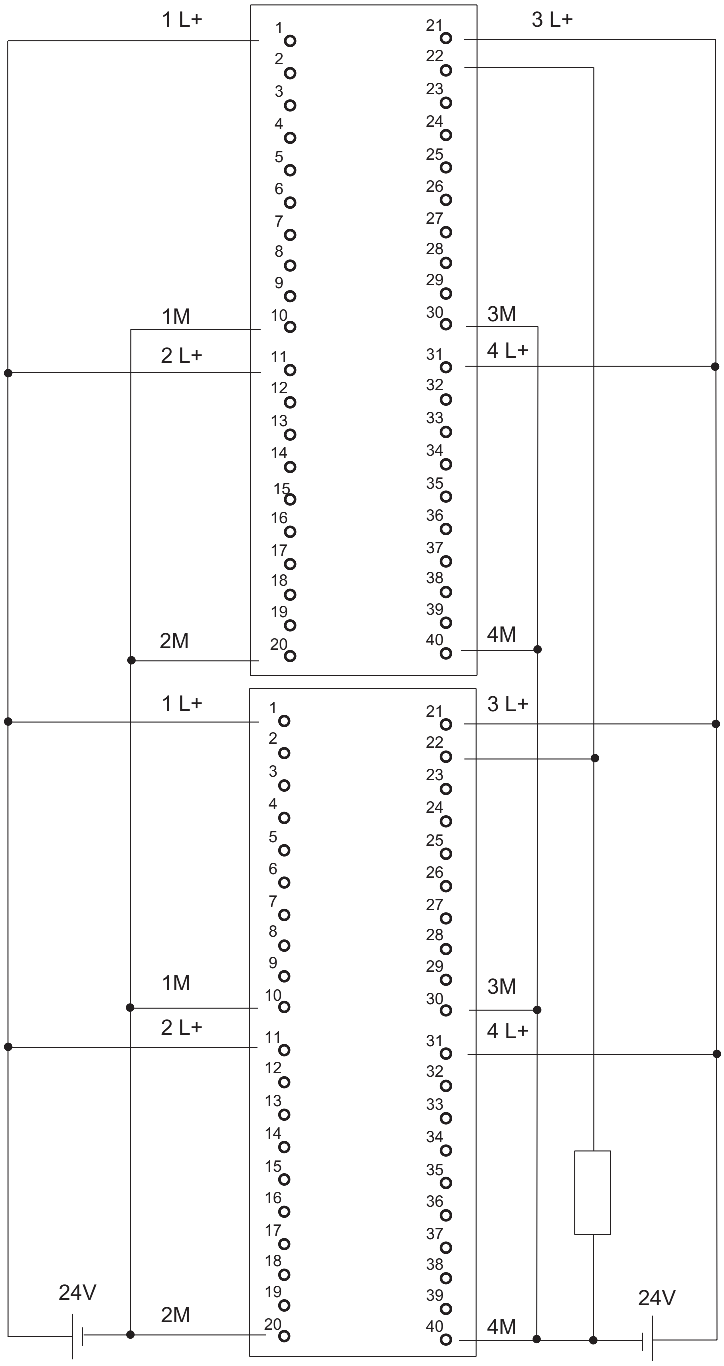


Figure F-20 Example of an interconnection with SM 322; DO 16 x DC 24 V/0.5 A

F.21 SM 332; AO 8 x 12 bit, 6ES7332–5HF00–0AB0

The diagram below shows the connection of two actuators to two redundant SM 332; AO 8 x 12 bit. The actuators are connected to channels 0 and 4. Suitable diodes include types of the series 1N4003 ... 1N4007, or any other diode with U_r >=200 V and I_F >= 1 A

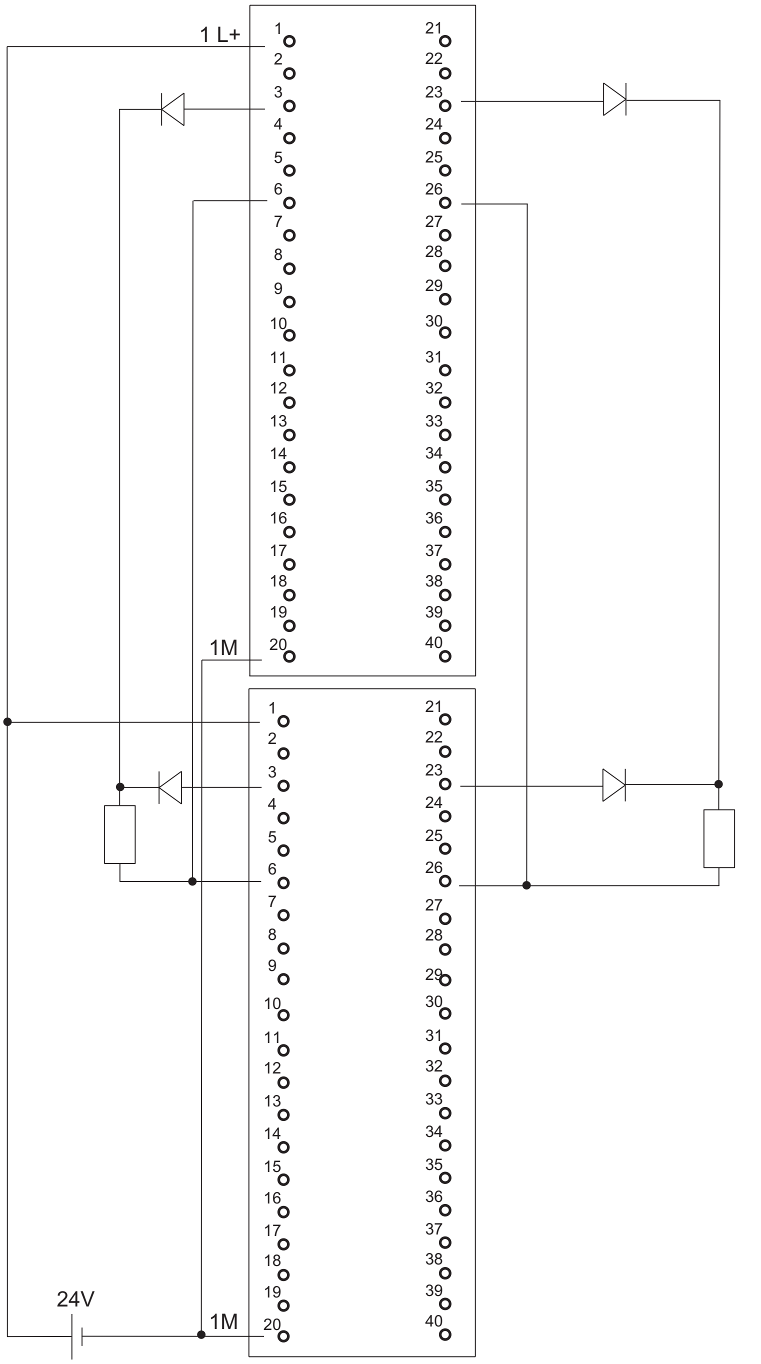


Figure F-21 Example of an interconnection with SM 332, AO 8 x 12 bit

F.22 SM 332; AO 4 x 0/4...20 mA [EEx ib], 6ES7332–5RD00–0AB0

The diagram below shows the connection of an actuator to two SM 332; AO 4 x 0/4...20 mA [EEx ib]. The actuator is connected to channel 0.
Suitable diodes include types of the series 1N4003 ... 1N4007, or any other diode with U_r >=200 V and I_F >= 1 A

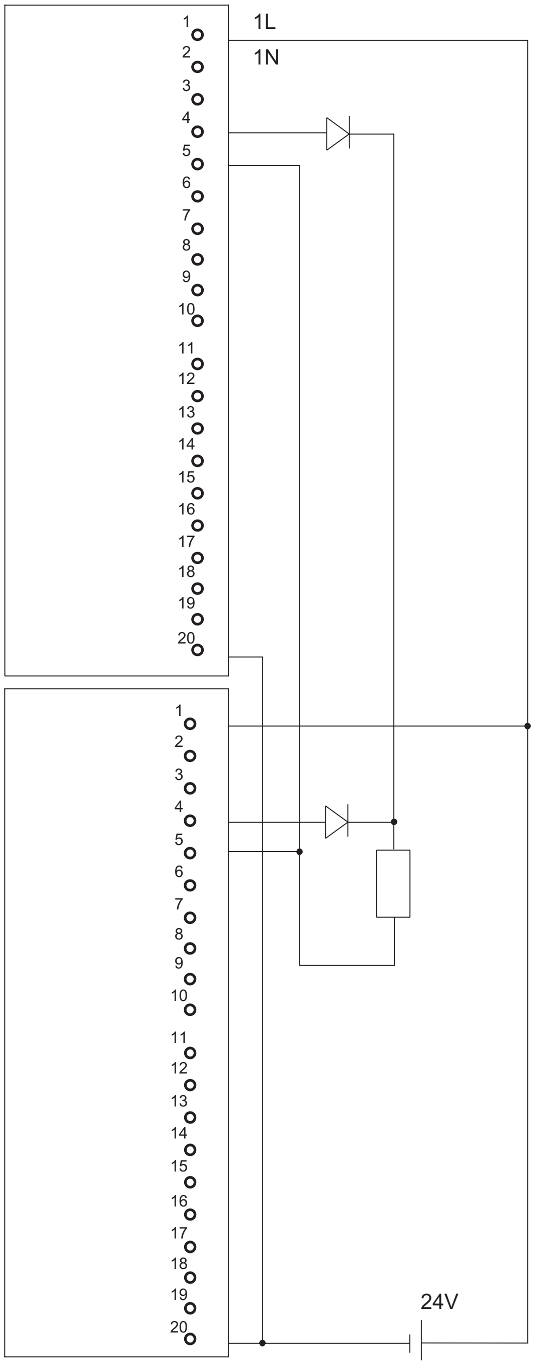


Figure F-22 Example of an interconnection with SM 332; AO 4 x 0/4...20 mA [EEx ib]

F.23 SM 422; DO 16 x AC 120/230 V/2 A, 6ES7422–1FH00–0AA0

The diagram below shows the connection of an actuator to two SM 422; DO 16 x 120/230 V/2 A. The actuator is connected to channel 0.

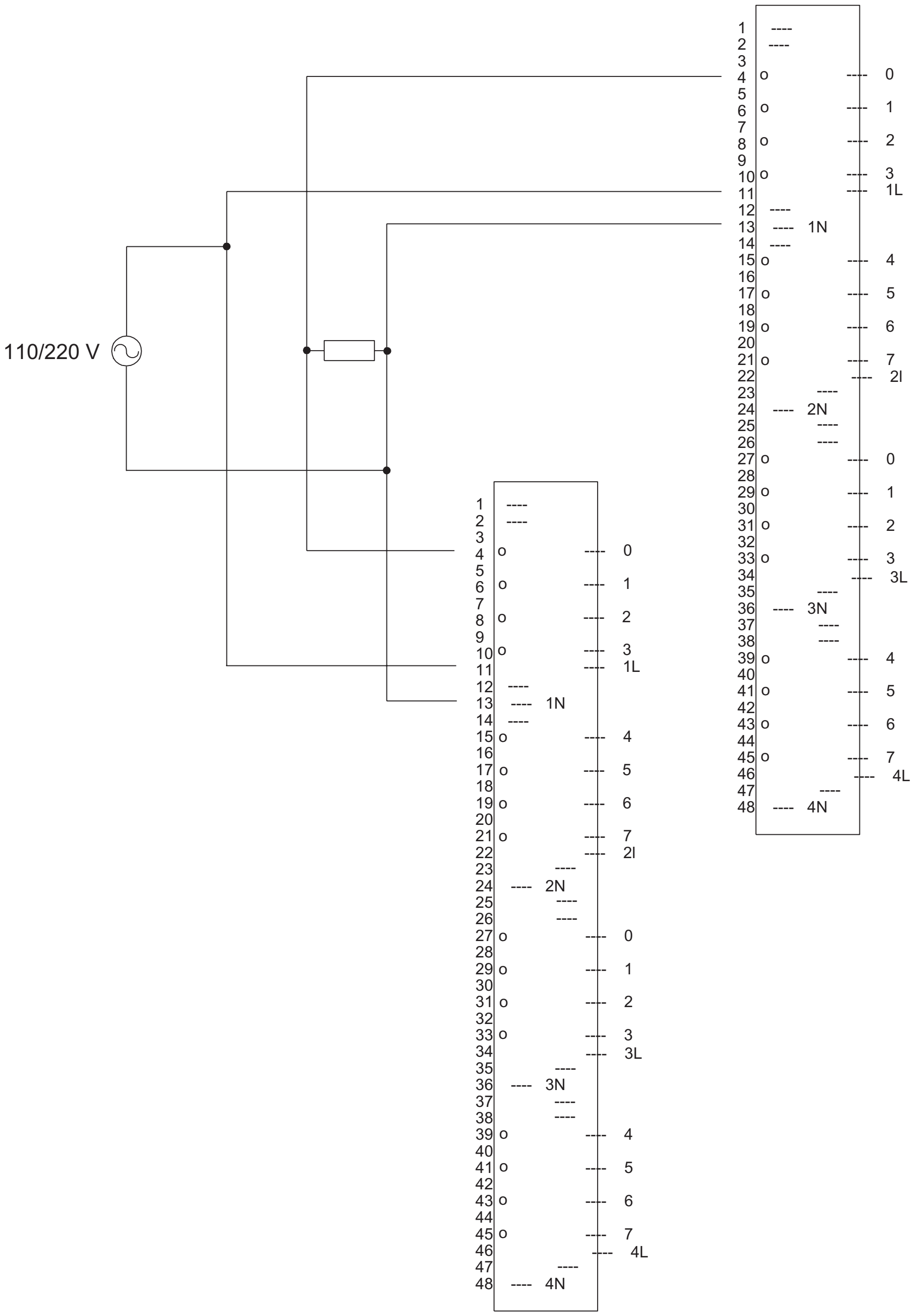


Figure F-23 Example of an interconnection with SM 422; DO 16 x 120/230 V/2 A

F.24 SM 422; DO 32 x DC 24 V/0,5 A, 6ES7422–7BL00–0AB0

The diagram below shows the connection of an actuator to two SM 422; DO 32 x 24 V/0.5 A. The actuator is connected to channel 0. Suitable diodes include types of the series 1N4003 ... 1N4007, or any other diode with U_r >=200 V and I_F >= 1 A

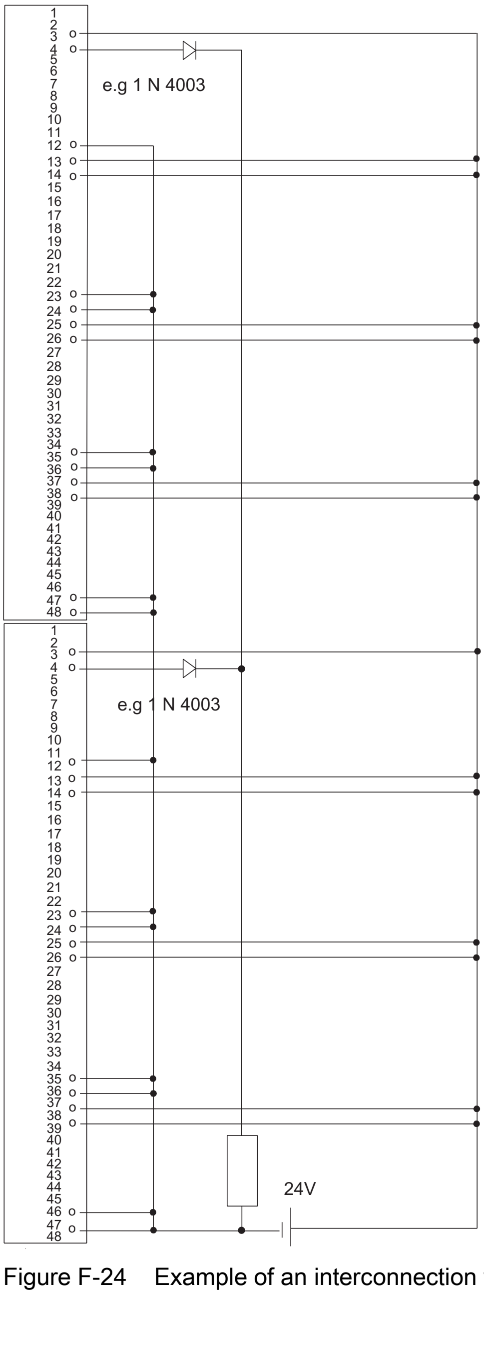


Figure F-24 Example of an interconnection with SM 422; DO 32 x DC 24 V/0.5 A

F.25 SM 331; AI 4 x 15 Bit [EEx ib]; 6ES7331–7RD00–0AB0

The diagram below shows the connection of a 2-wire measuring transducer to two SM 331; AI 4 x 15 bit [EEx ib]. The measuring transducer is connected to channel 1. Suitable Z diode BZX85C6v2 or 1N4734A.

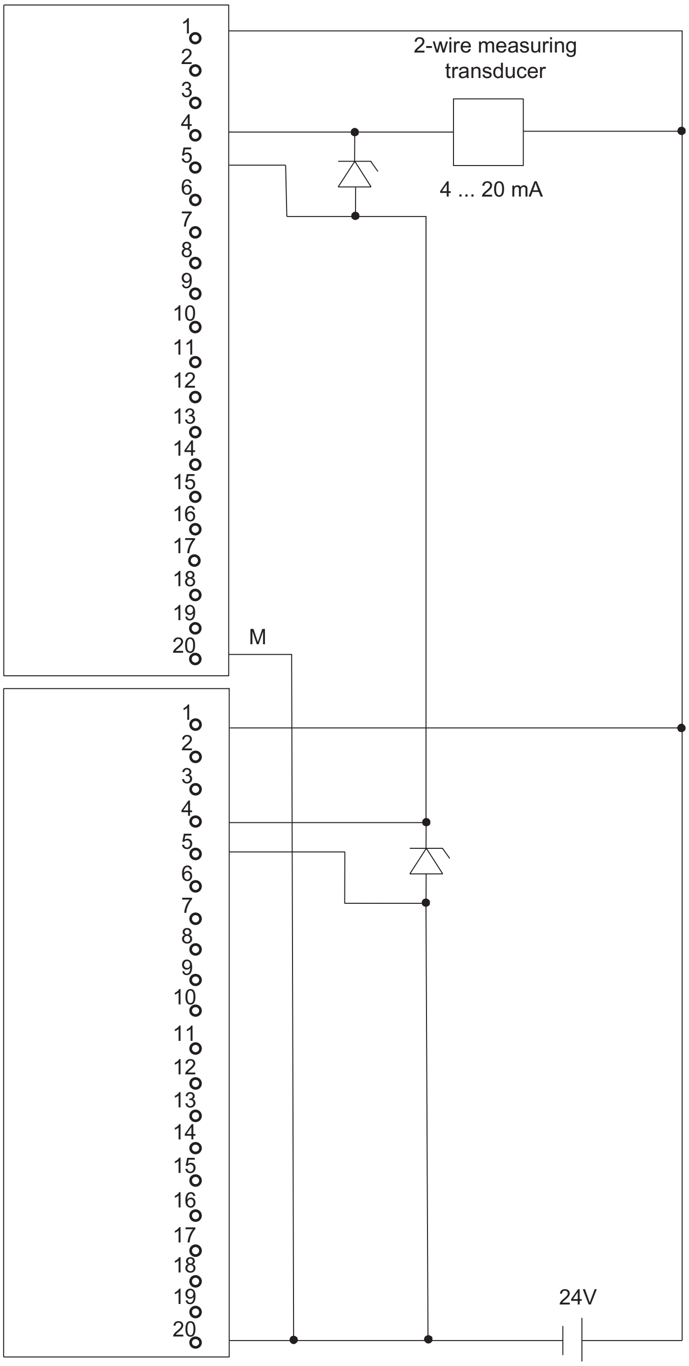


Figure F-25 Example of an interconnection with SM 331, AI 4 x 15 bit [EEx ib]

F.26 SM 331; AI 8 x 12 Bit, 6ES7331–7KF02–0AB0

The diagram below shows the connection of a measuring transducer to two SM 331; AI 8 x 12 bit. The measuring transducer is connected to channel 0.

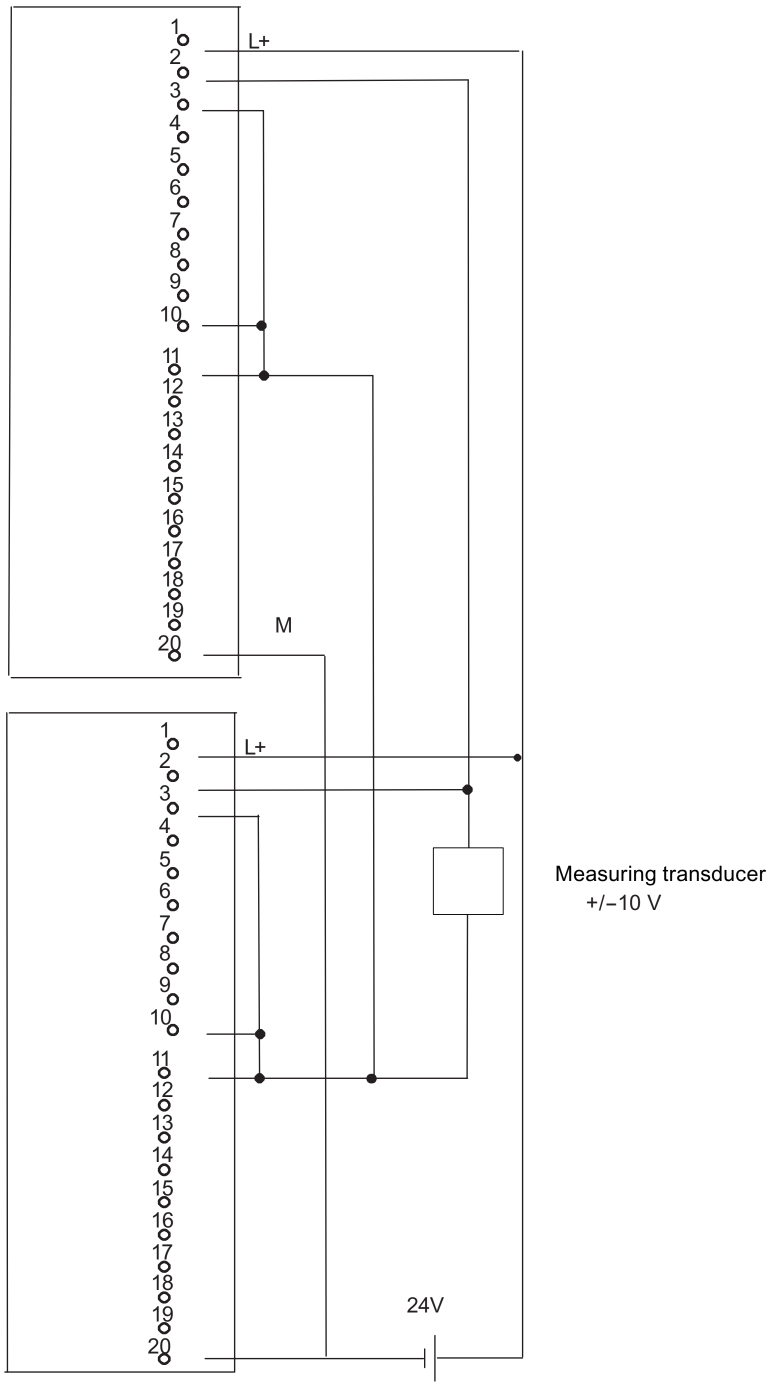


Figure F-26 Example of an interconnection with SM 331; AI 8 x 12 bit

F.27 SM 331; AI 8 x 16 Bit; 6ES7331–7NF00–0AB0

The figure below shows the connection of a measuring transducer to two redundant SM 331; AI 8 x 16 bit. The measuring transducer is connected to channel 0 and 7 respectively.

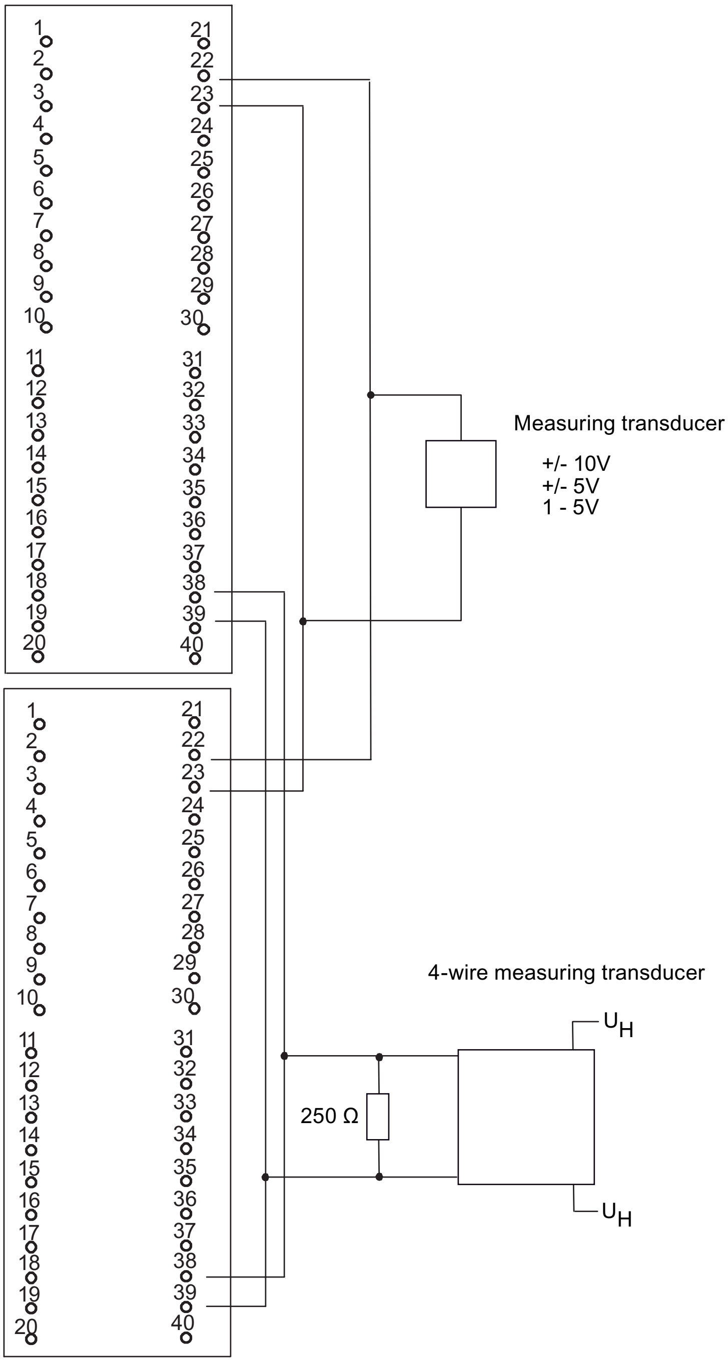


Figure F-27 Example of an interconnection with SM 331; AI 8 x 16 bit

F.28 SM 331; AI 8 x 16 Bit; 6ES7331–7NF10–0AB0

The figure below shows the connection of a measuring transducer to two redundant SM 331; AI 8 x 16 bit. The measuring transducer is connected to channel 0 and 3 respectively.

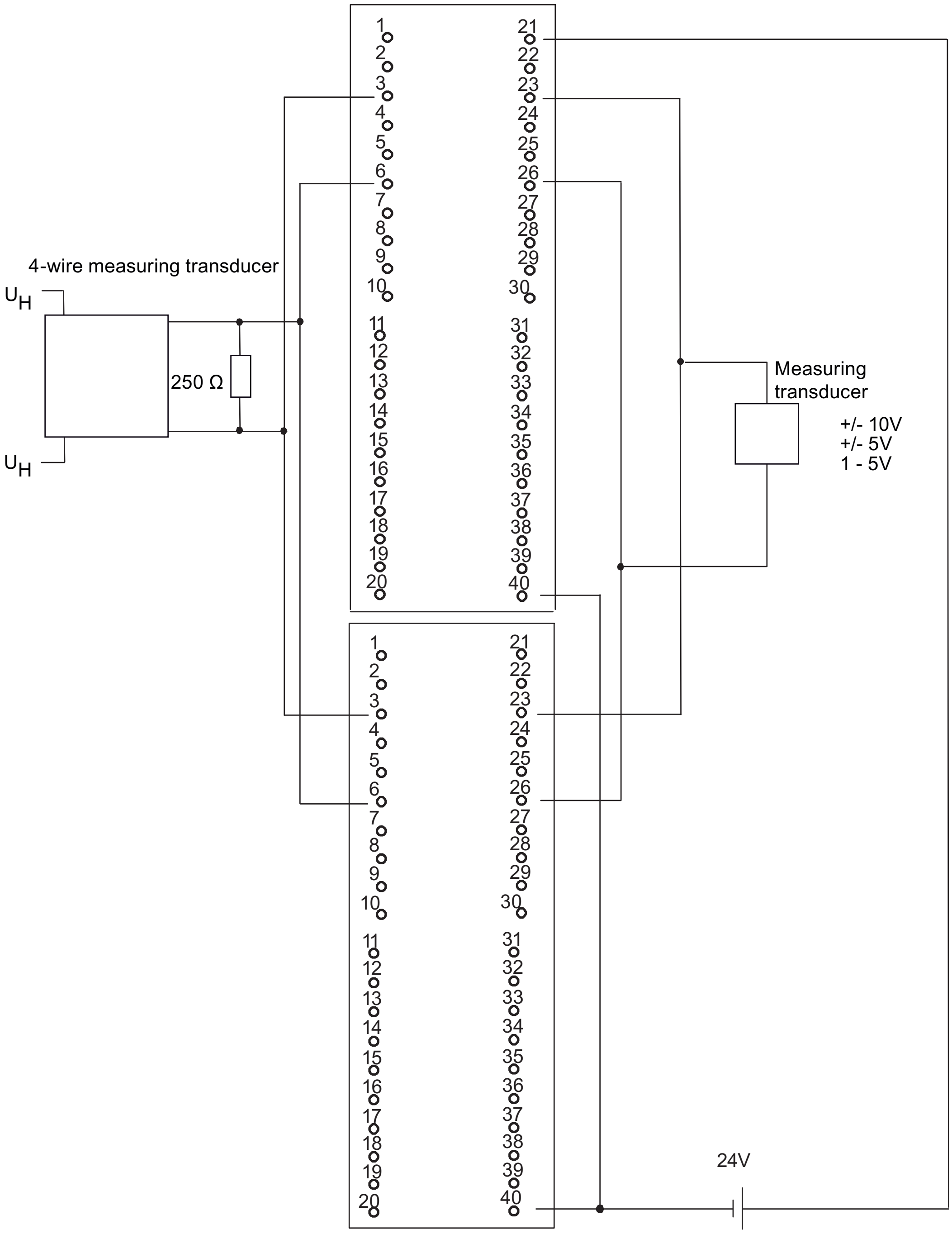


Figure F-28 Example of an interconnection with SM 331; AI 8 x 16 bit

F.29 AI 6xTC 16Bit iso, 6ES7331-7PE10-0AB0

The figure below shows the connection of a thermocouple to two redundant SM 331: AI 6xTC 16Bit iso.

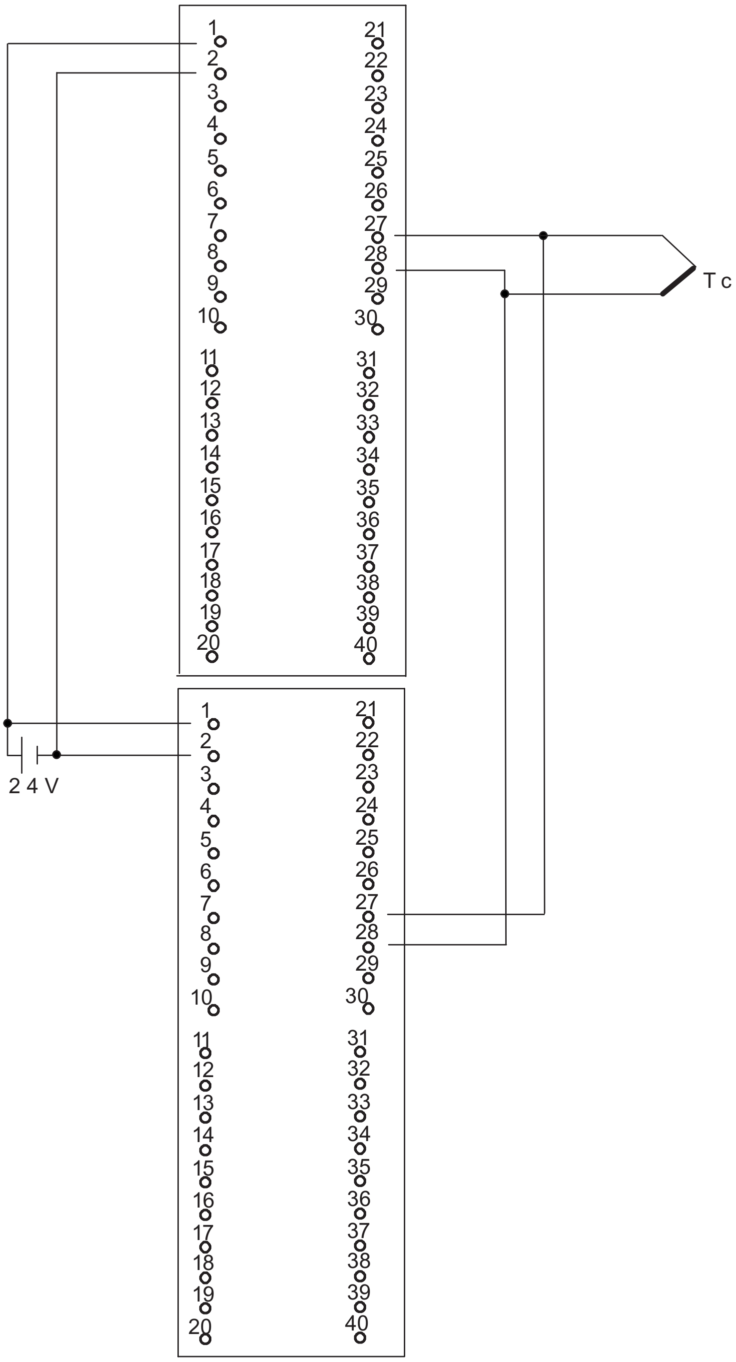


Figure F-29 Example of an interconnection AI 6xTC 16Bit iso

F.30 SM 331; AI 8 x 0/4...20mA HART, 6ES7331-7TF01-0AB0

The diagram below shows the connection of a 4-wire measuring transducer to two redundant SM 331; AI 8 x 0/4...20mA HART.

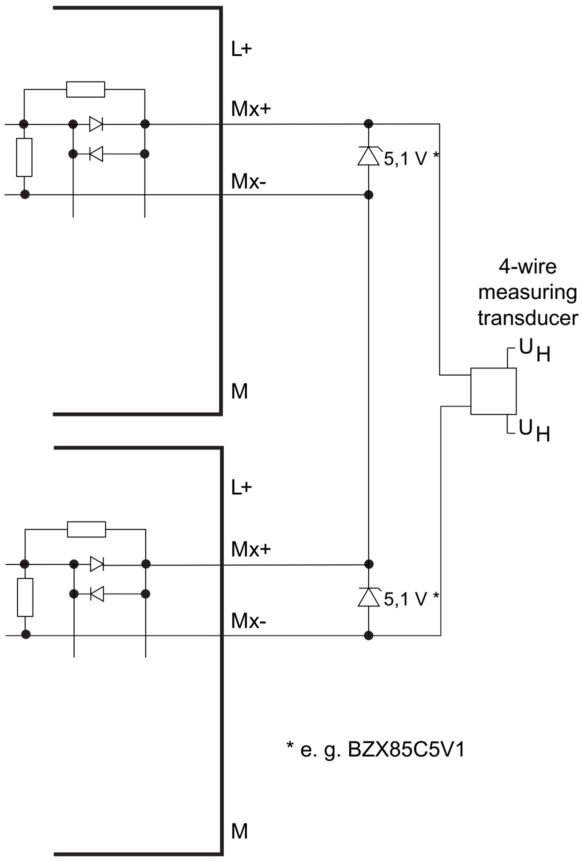


Figure F-30 Interconnection example 1 SM 331; AI 8 x 0/4...20mA HART

The diagram below shows the connection of a 2-wire measuring transducer to two redundant SM 331; AI 8 x 0/4...20mA HART.

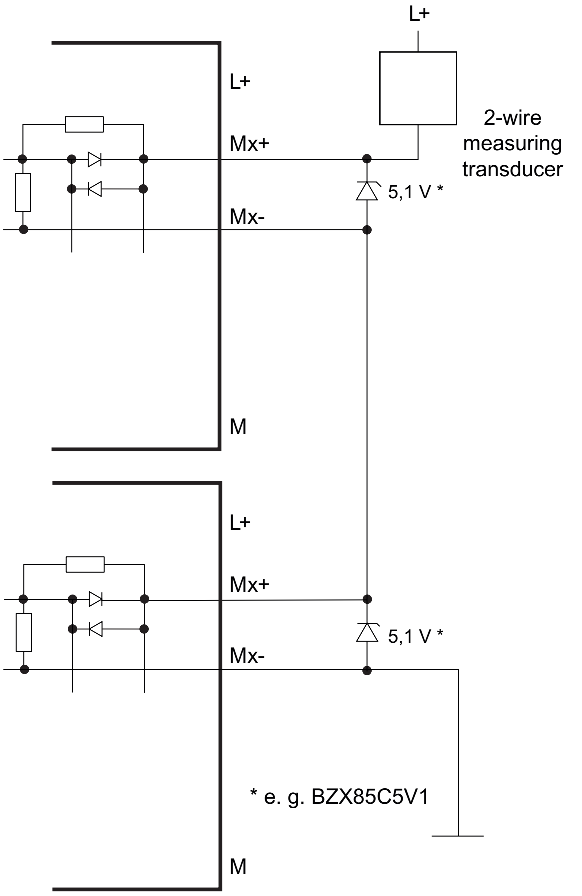


Figure F-31 Interconnection example 2 SM 331; AI 8 x 0/4...20mA HART

F.31 SM 332; AO 4 x 12 bit; 6ES7332–5HD01–0AB0

The diagram below shows the connection of an actuator to two SM 332; AO 4 x 12 bit. The actuator is connected to channel 0. Suitable diodes include types of the series 1N4003 ... 1N4007, or any other diode with U_r >=200 V and I_F >= 1 A

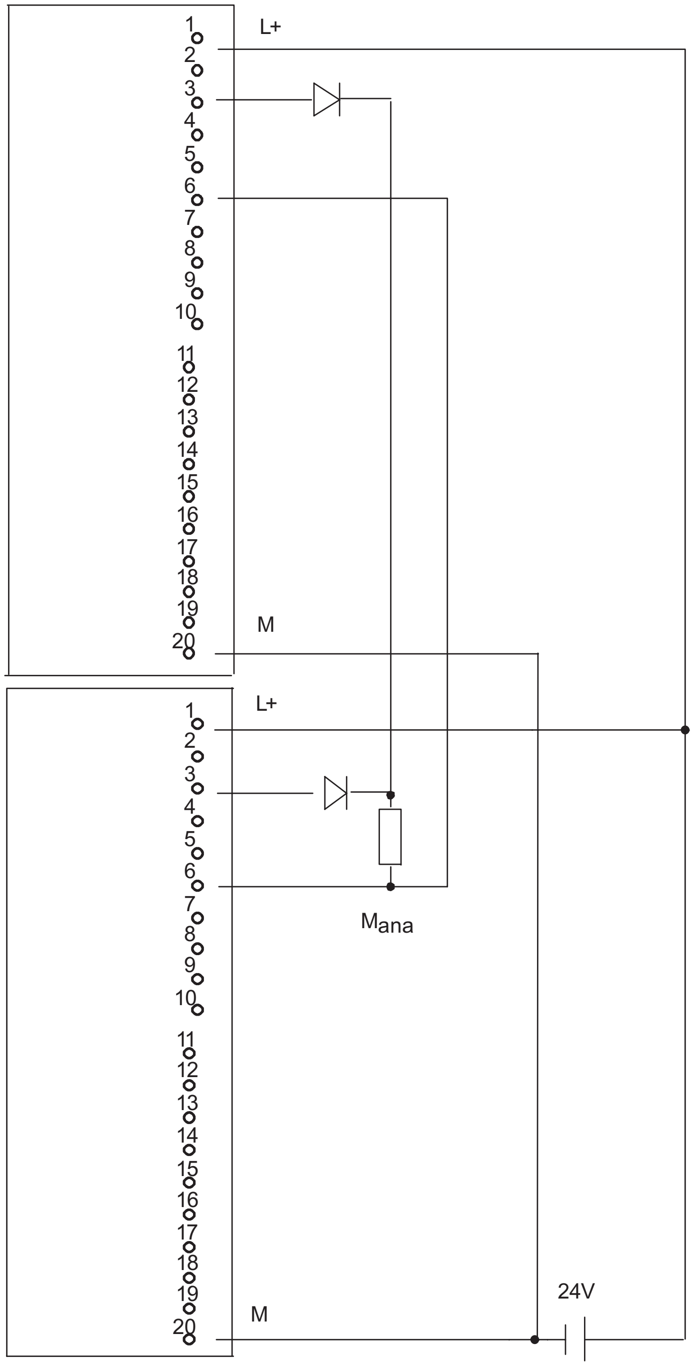


Figure F-32 Example of an interconnection with SM 332, AO 4 x 12 bit

F.32 SM 332; AO 8 x 0/4...20mA HART, 6ES7332-8TF01-0AB0

The diagram below shows the connection of an actuator to two SM 332; AO 8 x 0/4...20 mA HART.

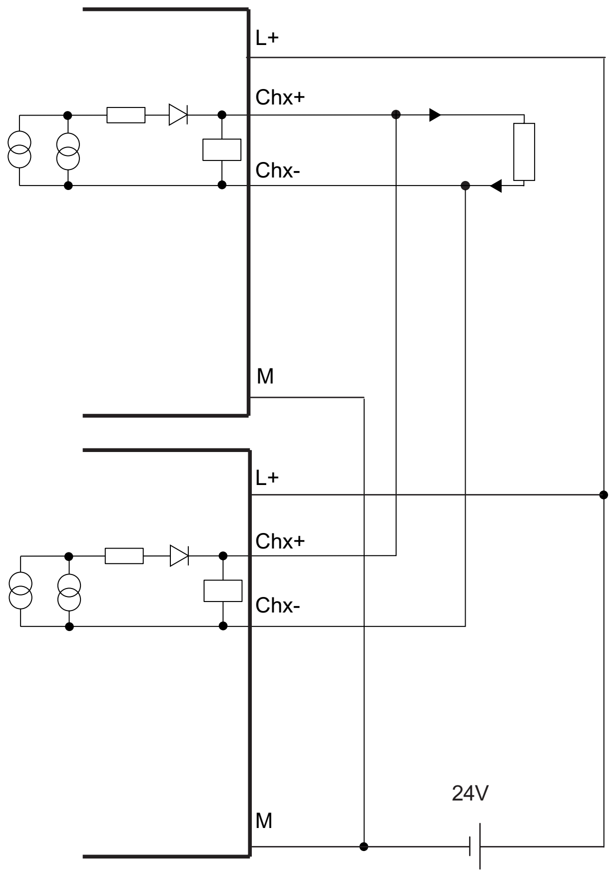


Figure F-33 Interconnection example 3 SM 332; AO 8 x 0/4...20mA HART

F.33 SM 431; AI 16 x 16 bit, 6ES7431–7QH00–0AB0

The diagram below shows the connection of a sensor to two SM 431; AI 16 x 16 bit. Suitable Z diode BZX85C6v2 or 1N4734A.

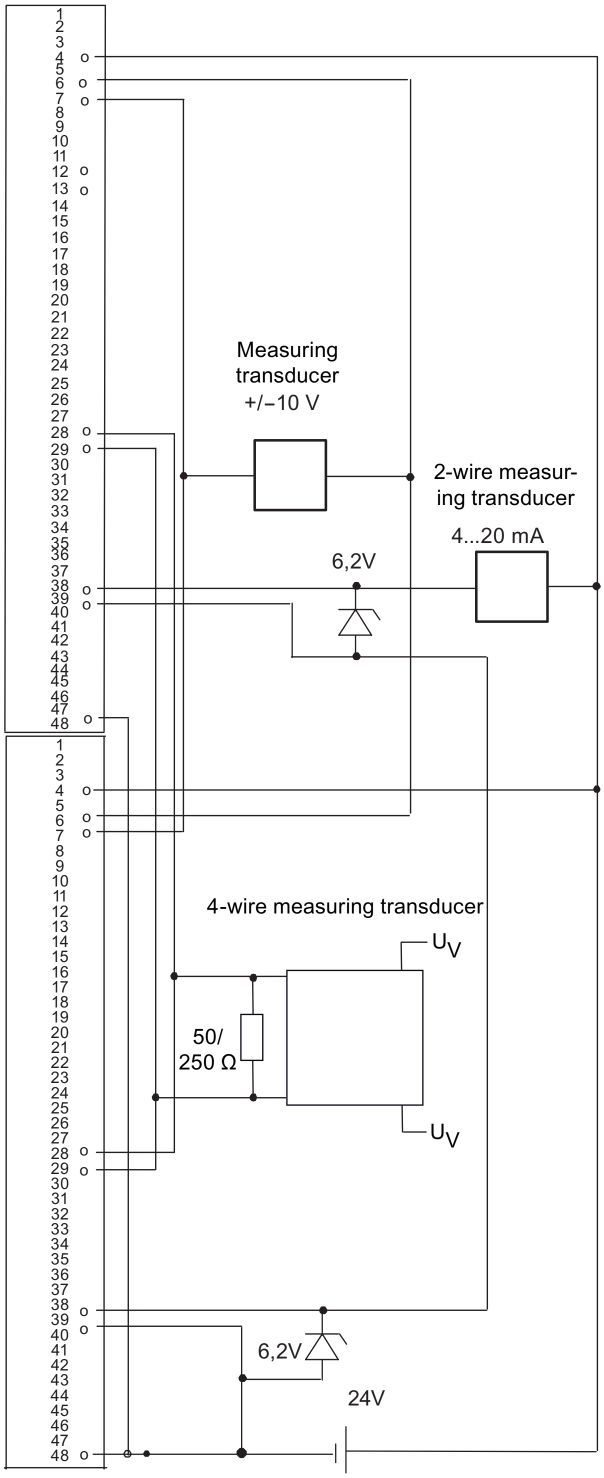


Figure F-34 Example of an interconnection with SM 431; AI 16 x 16 bit

Glossary

1-of-2 system

See Dual-channel H system

Comparison error

An error that may occur while memories are being compared on a fault-tolerant system.

Dual-channel H system

Fault-tolerant system with two central processing units

Fail-safe systems

Fail-safe systems are characterized by the fact that, when certain failures occur, they remain in a safe state or go directly to another safe state.

Fault-tolerant systems

Fault-tolerant systems are designed to reduce production downtime. Availability can be enhanced, for example, by means of component redundancy.

H station

A fault-tolerant 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 CPUs.

I/O, one-sided

We speak of a one-sided I/O when an input/output module can be accessed by only one of the redundant central processing units. It may be single-channel or multi-channel (redundant).

I/O, redundant

We speak of a redundant I/O when there is more than one input/output module available for a process signal. It may be connected as one-sided or switched. Terminology: "Redundant one-sided I/O" or "Redundant switched I/O"

I/O, single--channel

When there is only one input/output module for a process signal, in contrast to a redundant I/O, this is known as a single channel I/O. It may be connected as one-sided or switched.

I/O, switched

We speak of a switched I/O when an input/output module can be accessed by all of the redundant central processing units on a fault-tolerant system. It may be single-channel or multi-channel (redundant).

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.

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 CPUs.

Mean Down Time (MDT)

The mean down time MDT essentially consists of the time until error detection and the time required to repair or replace defective modules.

Mean Time Between Failures (MTBF)

The average time between two failures and, consequently, a criterion for the reliability of a module or a system.

Mean Time to Repair (MTTR)

The mean time to repair MTTR denotes the average repair time of a module or a system, in other words, the time between the occurrence of an error and the time when the error has been rectified.

Redundancy, functional

Redundancy with which the additional technical means are not only constantly in operation but also involved in the scheduled function. Synonym: active redundancy.

Redundant

In redundant system mode of a fault-tolerant system the central processing units are in RUN mode and are synchronized over the redundant link.

Redundant link

A link between the central processing units of a fault-tolerant system for synchronization and the exchange of data.

Redundant systems

Redundant systems are characterized by the fact that important automation system components are available more than once (redundant). When a redundant component fails, processing of the program is not interrupted.

Self-test

In the case of fault-tolerant CPUs defined self-tests are executed during startup, cyclical processing and when comparison errors occur. They check the contents and the state of the CPUs and the I/Os.

Single mode

An H system changes to single mode, when it was configured to be redundant and only one CPU is in RUN. This CPU is then automatically the master CPU.

Stand-alone operation

By stand-alone operation, we mean the use of a fault-tolerant CPU in a standard SIMATIC-400 station.

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 CPUs.

Stop

With fault-tolerant systems: In the Stop system mode of a fault-tolerant system the central processing units of the fault-tolerant system are in STOP mode.

Synchronization module

An interface module to the redundant link on a fault-tolerant system.

TROUBLESHOOTING

An operating mode of the standby CPU of a fault-tolerant system in which the CPU performs a complete self-test.

Update

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

Index

4

41xH CPU
    DP address areas, 68
    DP master: diagnostics with LEDs, 71

A

A&D Technical Support, 19
Address area
    41xH CPU, 68
Analog output signals, 161
Applied value, 155
Availability
    Communication, 31
    Definition, 353
    I/O, 129
    of systems, 23

B

Base system, 28
Bumpless continuation, 85
Bus connectors, 58
    MPI, 57
    PROFIBUS DP interface, 58
Bus interruption, 75
Bus topology, 70
BUSF, 71
BUSF1, 47
BUSF2, 47

C

Central module, 28
Change memory type, 268
Checksum errors, 95
Cold restart, 52
    Operating sequence, 53
Commissioning, 35
    Requirements, 35
Commissioning the S7-400H, 37
Communication, 31
Communication blocks
    Consistency, 77
Communication functions, 109
Communication processors, 373
Communication via MPI and communication bus
    Cycle load, 294
Comparison error, 95
Components
    Base system, 28
    Duplicating, 23
Configuration, 31
Configuration, 25
configuring, 194
Configuring networking, 198
Connection
    Fault-tolerant S7, 172
    S7, 171
Consistent data, 76
Consistent data access, 80
CPU
    Mode selector switch, 49
    Parameters, 59
CPU 412-3H
    Operator controls and indicators, 39
CPU 414-4H
    Operator controls and indicators, 40
CPU 417-4H
    Operator controls and indicators, 40
CPU memory reset
    Operating sequence, 51
    Process, 51
CPU redundancy errors, 33
CPU-CPU communication, 57
Cycle control
    Execution time, 298
Cycle load
    Communication via MPI and communication bus, 294
Cycle time, 292
    Elements, 293
    Extending, 294
Cyclic self-test, 96

D

Data consistency, 76
Determining memory requirements, 56
SM 321
  Example of an interconnection, 377
SM 321
  Example of an interconnection, 375
SM 321
  Example of an interconnection, 376
SM 321
  Example of an interconnection, 378
Diagnostic addresses for PROFIBUS, 74
Diagnostic buffer, 48
Diagnostics
  Evaluating, 73
Diagnostics addresses, 74
Digital output
  Fault-tolerant, 154, 161
Diode circuit, 161
Direct current measurement, 159
Discrepancy
  Digital input modules, 152
Discrepancy time, 152, 155
SM 422
  Example of an interconnection, 397
SM 322
  Example of an interconnection, 389
SM 322
  Example of an interconnection, 388
Documentation, 34
DP interface, 58
DP master
  Diagnostics using LEDs, 71
  Diagnostics with STEP 7, 72
DP master system
  Startup, 69
DPV1, 69
DPV1 and EN 50170, 70
DPV1 master, 69
DPV1 mode, 70
DPV1 slaves, 69

E

EN 50170, 69
Encoder
  Double redundant, 154
Error displays
  All CPUs, 47
  CPU 414-4H, 48
  CPU 417-4H, 48
Error LEDs
  Synchronization module, 281
Error messages, 44
Execution time
  Cycle control, 298
  Operating system, 298
  Process image update, 295
  User program, 294
Expanded memory configuration, 106
Expanding load memory, 54
External backup voltage, 42
External diodes, 155
EXTF, 47

F

Fail-safe, 21
Failure of a CPU, 38
Failure of a fiber-optic cable, 38
Failure of a power supply module, 38
Failure of a redundancy node, 24
Failure of components, 201
  in central and expansion racks, 202
  of distributed I/Os, 213
Fault-tolerant, 21
Fault-tolerant communication, 170
Fault-tolerant connections
  Configuration, 174
  Programming, 175, 182
  Properties, 174
Fault-tolerant station, 194
FB 450 RED_IN, 142
FB 451 RED_OUT, 142
FB 452 RED_DIAG, 142
FB 453 RED_STATUS, 142
FC 450 RED_INIT, 142
FC 451 RED_DEPA, 142
Fiber-optic cables, 29
  Cable pull-in, 284
  Installation, 283
  Replacement, 208
  Selection, 285
  Storage, 283
Finding your way
  through the manual, 17
Firmware
  Updating, 61
FLASH card, 54, 55
FRCE, 47
Function modules, 373
Functional I/O redundancy, 142

H

H system
Starting, 37
Hardware
Components, 28
Configuration, 37
Configuring, 196
Installation, 36
HOLD, 92
Hot restart
Operating sequence, 53
Hotline, 19

I

I/O, 30, 129
Configuration versions, 30
one-sided, 131
Redundant, 138
Switched, 133
I/O direct access, 97, 308
I/O redundancy errors, 33
IFM1F, 47
IFM2F, 47
Indirect current measurement, 157
Installation, 25
Installation types
I/O, 129
INTF, 47

L

LED
BUSF, 71
LED display, 41
Link-up, 99, 100, 101, 105, 113, 117, 168
Flow chart, 102
Monitoring times, 168
Sequence, 105
Time-based reaction, 117
LINK-UP, 90
Link-up and update
Disabling, 113
Effects, 99
Sequence, 101
Starting, 101
Link-up with master/standby changeover, 105
Link-up, Update, 91
Load memory, 110
Loss of redundancy, 85

M

Master CPU, 84
Master/standby assignment, 84
Maximum communication delay
Calculation, 123
Definition, 114
Maximum cycle time extension
Calculation, 124
Definition, 114
Maximum disable time for priority classes > 15
Calculation, 120
Maximum inhibit time for priority classes > 15
Definition, 114
MDT, 349
Memory card, 54
Function, 54
Memory card slot, 41
Memory expansion, 266
Memory reset, 89
Message functions, 108
Minimum I/O retention time
Calculation, 119
Definition, 115
Mode selector switch, 41, 49
Monitoring functions, 44
Monitoring times, 114
Accuracy, 118
Configuration, 118
MPI interface, 57
MPI parameters, 52
MPI/DP interface, 42
MSTR, 46
MTBF, 349, 354
Multiple-bit errors, 96

N

Network configuration, 198
Non-redundant encoders, 153, 156

O

OB 121, 94
Online help, 17
Operating mode
Changing, 364
Operating mode changes, 75
Operating objectives, 21

Operating states
- CPU, 88
- HOLD, 92
- LINK-UP, 90
- RUN, 91
- STARTUP, 90
- STOP, 89
- System, 87
- UPDATE, 90

Operating system
- Execution time, 298

Order numbers
- Memory card, 345

Organization blocks, 33

P

Parameter assignment tool, 60
Parameter block, 59
Parameters, 59
PG functions, 199
PG/OP - CPU communication, 57
Power supply, 28
Process image update
- Execution time, 295

Process interrupt
- in the S7-400H system, 97

Process interrupt processing, 315
Process interrupt reaction time
- of signal modules, 315
- of the CPUs, 314

PROFIBUS address, 69
PROFIBUS DP interface, 42
Programming, 31
Programming via PROFIBUS, 69

R

Rack number
- Setting, 42

RACK0, 46
RACK1, 46
Racks, 28
RAM, 111
RAM card, 54, 55
RAM/PIO comparison error, 95
Reaction time, 97
- Calculation of the, 306, 307
- Elements, 304
- Longest, 307
- Reducing, 308
- Shortest, 306

Reaction to timeouts, 116
Reading data consistently from a DP standard slave, 79
REDF, 48
Redundancy
- Active, 84
- Functional, 84

Redundancy nodes, 24, 170
Redundant analog output modules, 161
Redundant automation systems, 21
Redundant communication system, 170
Redundant encoders, 154
- Analog input modules, 160

Redundant I/O, 22, 138
- Analog input modules, 155
- Configurations, 138
- Digital input modules, 152
- Digital output modules, 154
- in central and expansion units, 138
- in single mode, 141
- in the one-sided DP slave, 139
- in the switched DP slave, 140
- Project engineering, 145

Redundant mode, 91
Reliability, 349
Repair, 201
Replacement in operation, 201
- in central and expansion racks, 202
- of distributed I/Os, 213

Restart, 52
- Operating sequence, 53

Rocker switch, 49
Rules for assembly, 27, 195
RUN, 46, 91

S

S5 to S7
- Configuration, 368
- Diagnostics and programming, 368

S7 connections
- Configured, 171, 175

S7-400
- Optional software, 32

S7-400H
- Communication, 31
- Configuration and programming, 32
- Documentation, 34
- I/O, 30
- User program, 33

S7-400H
- Blocks, 33

S7-compatible mode, 70
S7-REDCONNECT, 174, 187
Save service data, 65
Scope
- of the manual, 15

Security level, 50
- Setting, 50

Self-test, 86, 94
SFB 14, 78
SFB 15, 78
SFC 103 DP_TOPOL, 70
SFC 109 PROTECT, 50
SFC 14 DPRD_DAT, 79
SFC 15 DPWR_DAT, 79
SFC 81 UBLKMOV, 76
Signal modules for redundancy, 146
SIMATIC Manager, 199
Single mode, 91
Single-bit errors, 96
Single-channel one-sided I/O, 131
- Failure, 132

Single-channel switched I/O, 133
Single-channel, switched I/O
- Failure, 135

Slot for interface modules, 41
Software
- Redundancy, 22

Stand-alone operation
- Configuring, 363
- Definition, 361
- Points to note, 362
- to a fault-tolerant system, 363

Standby CPU, 84
- Startup, 90

Startup modes, 90
Startup monitoring, 69
Startup processing, 90
Status byte, 163
Status displays
- All CPUs, 46
- CPU 414-4H, 46
- CPU 417-4H, 46

Status word, 163
STOP, 46
Subconnection
- Active, 172

Switch to CPU with expanded memory configuration, 111
Switch to CPU with modified configuration, 110
Synchronization, 85
- Event-driven, 85

Synchronization module
- Function, 279
- Replacement, 208

Synchronization modules, 29
System modifications during operation
- Hardware requirements, 366
- Software requirements, 366
- Stand-alone operation, 365

System states, 87

T

Technical specifications
- Memory card, 345

Technical support, 19
Time monitoring, 114
Time-based reaction, 97, 126
Timeout, 116
Tolerance window, 155
Tools, 32

U

Update, 99, 100, 101, 113, 117, 168
- Delay, 126
- Minimum input signal duration, 104
- Monitoring times, 168
- Sequence, 107
- Time-based reaction, 117

UPDATE, 90
Updating online
- the firmware, 61

Updating the firmware, 61
Usable CPs, 174
User program, 33
User program execution time, 294

W

Warm restart, 52
Writing data consistently to a DP standard slave, 79