
Contents

| | |
|---|----|
| 1 Introduction | 1 |
| 1.1 Preface | 1 |
| 1.2 Who is this book suitable for? | 1 |
| 1.3 How to read this book | 1 |
| 1.4 Definition of key terms | 3 |
| 1.5 Installing the WinPLC7 V4 Demo Version | 4 |
| 1.6 Installing WinPLC7 V4 as Standard Version | 5 |
| 2 PLC Technical Basics | 6 |
| 2.1 What is a Programmable Logic controller? | 6 |
| 2.2 What changes by using a PLC? | 8 |
| 2.3 Setup of a Programmable Logic Controller | 9 |
| 2.4 How to program and control a PLC | 10 |
| 2.5 Examples of a plant with a PLC | 12 |
| 2.6 The PLC-functions with STEP®7 | 15 |
| 2.6.1 Block Status | 15 |
| 2.6.2 Status-Variable | 15 |
| 2.6.3 Control-Variable | 16 |
| 2.6.4 Module state | 16 |
| 2.6.5 Overview of the CPU-Functions (Protocols) | 18 |
| 3 The first S7-Program | 19 |
| 4 Explanation of the operands in STEP®7 | 29 |
| 4.1 Input and Output Operands | 29 |
| 4.2 Bit Memory Operand | 29 |
| 4.3 Local Operands | 29 |
| 4.4 Data of a Block Data | 30 |
| 4.5 Timers | 30 |
| 4.6 Counters | 30 |
| 4.7 Periphery Inputs | 30 |
| 4.8 Periphery Outputs | 30 |
| 4.9 Overview of Operands | 31 |
| 5 Addressing Operands | 32 |
| 5.1 Notation of Bit Operands | 32 |

| | |
|---|-----------|
| 5.2 Notation of Byte Operands | 33 |
| 5.3 Notation of Word Operands | 34 |
| 5.4 Notation of Double Word Operands | 35 |
| 5.5 Important Usage Notes on Addressing | 36 |
| 6 Symbolic Programming | 37 |
| 6.1 How to create a Symbolic File | 38 |
| 6.2 Enable the Symbolic within the Programming Software | 40 |
| 6.3 Using Symbols when programming | 40 |
| 6.4 Difference between Symbol and Variable | 41 |
| 7 Logic Operations | 42 |
| 7.1 AND Operation | 43 |
| 7.2 OR Operation | 44 |
| 7.3 EXCLUSIVE OR Operation | 45 |
| 7.4 Logical Negation | 46 |
| 7.4.1 Exercise: Logical Negation | 47 |
| 7.5 NAND Operation | 48 |
| 7.6 NOR Operation | 49 |
| 7.7 Result of Logic Operation (RLO) | 50 |
| 7.8 Combined AND/OR Functions without bracketed operations | 53 |
| 7.8.1 Exercise: AND/OR combined | 54 |
| 7.9 Bracketed Operations | 55 |
| 7.9.1 Exercise: Bracketed Operation | 57 |
| 7.10 OR operation of AND operations | 58 |
| 7.11 Set-Reset Instructions (flipflop) | 59 |
| 7.11.1 Exercise: flipflop | 63 |
| 8 Linear and structured Programming | 64 |
| 8.1 Linear Programming | 64 |
| 8.2 Structured Programming | 78 |
| 8.2.1 Organization Blocks (OB) | 78 |
| 8.2.2 The Function (FC) | 80 |
| 8.2.3 The Function block (FB) | 80 |
| 8.2.4 The Data Block (DB) | 81 |
| 8.2.5 System Functions (SFC) and System Function Blocks (SFB) | 81 |
| 8.2.6 The System Data Block (SDB) | 82 |

| | |
|--|------------|
| 8.2.7 Maximum Number of User Blocks | 82 |
| 8.2.8 Calling a Function FC | 83 |
| 8.2.9 Call of an FB | 86 |
| 8.2.10 Instructions required for ending a Block | 87 |
| 8.2.11 Example for Structured Programming | 90 |
| 9 Data types in STEP®7 | 102 |
| 9.1 Elementary Data Types | 104 |
| 9.2 Complex Data Types | 105 |
| 9.3 Parameter Types | 105 |
| 10 Load and Transfer instructions | 106 |
| 10.1 Loading Bytes | 106 |
| 10.2 Loading Words | 107 |
| 10.3 Loading double words | 108 |
| 10.4 Note of caution concerning word operations | 109 |
| 10.5 Loading constants | 110 |
| 11 Block parameter | 114 |
| 11.1 Example for Block Parameters | 114 |
| 11.1.1 Defining the Declaration Areas | 116 |
| 11.1.2 Assigning the Parameters to the Declaration Areas | 117 |
| 11.1.3 Programming the Block Parameters | 117 |
| 11.2 Processing the Formal Parameters | 129 |
| 11.2.1 Accessing Formal Parameters of the Data Type BOOL | 129 |
| 11.2.2 Write Access to a BOOL Input Parameter | 130 |
| 11.2.3 Accessing Formal Parameters with digital Data Types | 131 |
| 11.2.4 Example for Parameter with a digital Data Type | 132 |
| 11.2.5 Accessing Formal Parameters with complex Data Types | 135 |
| 11.2.6 Example for Parameter with Data Type Array | 136 |
| 11.2.7 Declaration of a STRUCT | 140 |
| 11.2.8 Examples for the Data Type STRUCT | 141 |
| 11.2.9 Declaration of a STRING | 147 |
| 11.2.10 Declaration of a DATE_AND_TIME | 149 |
| 12 Global Data Blocks | 150 |
| 12.1 Creating a DB | 150 |
| 12.2 Accessing a DB | 155 |
| 12.2.1 Accessing a Data Bit | 156 |

| | |
|---|------------|
| 12.2.2 Accessing a Data Byte, Data Word and Data Double Word | 156 |
| 12.2.3 Accessing the Data of a DB via the Notation of the Variables | 156 |
| 12.3 The Difference between Initial and Actual Value | 159 |
| 12.3.1 How to set Actual Values to Initial Values | 164 |
| 12.4 Instructions and Functions in Connection with Data Blocks | 165 |
| 12.4.1 Opening a Data Block | 165 |
| 12.4.2 How to determine the Length of a Data Block | 166 |
| 12.4.3 Determining the Number of the Opened Data Block | 169 |
| 12.4.4 Creating and Testing a Data Block | 170 |
| 12.4.5 How to delete a Data Block | 175 |
| 12.4.6 Pre-Allocation of the Data Type ARRAY | 181 |
| 12.4.7 Pre-Allocation of the Data Type STRING | 184 |
| 12.4.8 Write Protection for a Data Block | 185 |
| 12.4.9 How to store a Data Block within the Load Memory | 186 |
| 12.4.10 Possible Number of DBs within a CPU | 187 |
| 13 Function Blocks | 188 |
| 13.1 Block Characteristics | 188 |
| 13.2 Example for Function Blocks | 188 |
| 13.2.1 Creating the PLC Program | 189 |
| 13.3 Call of a Function Block without the Indication of Actual Parameters | 205 |
| 13.4 The Difference between Instance Data Block and Global Data Block | 211 |
| 13.4.1 The DI-Register | 211 |
| 13.5 The Static Local Data | 212 |
| 14 Counter | 213 |
| 14.1 Setting and Resetting a Counter | 213 |
| 14.2 Testing a Counter | 214 |
| 14.3 Loading a Counter with a Count Value | 214 |
| 14.3.1 Loading a Constant Count Value | 215 |
| 14.3.2 Additional Methods of Pre-allocating a Counter | 215 |
| 14.4 Up Counter | 216 |
| 14.5 Down Counter | 217 |
| 14.6 Example for a Counter | 218 |
| 14.7 Another Example for a Counter | 219 |
| 14.8 The Number of Available Counters | 223 |
| 14.9 Binary Counter Test | 223 |

| | |
|--|-----|
| 15 Timer | 224 |
| 15.1 Loading a Timer Function with a Time Value | 224 |
| 15.1.1 Loading a Time via a Constant Time Value | 225 |
| 15.1.2 Additional methods of loading a Time Constant | 226 |
| 15.2 Starting and Resetting of a Time | 227 |
| 15.3 Time Test | 227 |
| 15.4 The Timer Type SP (Pulse) | 228 |
| 15.5 The Timer Type SE (Extended Pulse Timer) | 229 |
| 15.6 The Timer Type SD (Switch-on Delay Timer) | 230 |
| 15.7 The Timer Type SS (Retentive On-Delay Timer) | 231 |
| 15.8 The Timer Type SF (Switch-off Delay Timer) | 232 |
| 15.9 Example for Timers | 233 |
| 15.10 Another Example for Timers | 234 |
| 15.11 Timers as Block Parameters | 241 |
| 15.12 Number of the Available Timers | 243 |
| 15.13 Important Note about Timers | 243 |
| 15.14 Edge Evaluation | 244 |
| 15.14.1 Example of a "Positive Edge" | 245 |
| 15.14.2 Negative Edge | 245 |
| 15.15 Binary Down Scaler (T-Flip-Flop) | 246 |
| 16 Sequencer Programming (Sequential Control) | 248 |
| 16.1 Task | 248 |
| 16.2 Separating the complete Procedure into individual Steps | 249 |
| 16.3 Assignment of Input and Output | 250 |
| 16.4 Creating the Program | 251 |
| 16.5 Testing the PLC Program | 260 |
| 17 The Registers of the CPU | 264 |
| 17.1 Accumulators | 264 |
| 17.2 Address Register | 264 |
| 17.3 DB Register | 265 |
| 17.4 The Status Word | 265 |
| 18 Processing the S7-Program within the PLC | 266 |
| 18.1 The Operating Modes of a PLC | 266 |

| | |
|---|------------|
| 18.2 The Process Image | 269 |
| 19 Jump Instructions | 271 |
| 19.1 Syntax of the Jump Instructions | 272 |
| 19.2 Unconditional Jump (JU) | 272 |
| 19.3 Jump Instructions that evaluate the RLO | 273 |
| 19.4 Jump Instructions that evaluate the Binary Result | 274 |
| 19.5 Jump Instructions that evaluate the Statusword Bits (CC0, CC1) | 275 |
| 19.6 Jump Instruction in Overflow Conditions | 278 |
| 19.7 The LOOP Instruction | 279 |
| 19.8 Branch Destination List, Jump List (JL) | 280 |
| 19.9 Direct Evaluation of the Status Word | 282 |
| 20 Error diagnostic within an S7-CPU | 283 |
| 20.1 Error Detection via Diagnostic Buffers | 284 |
| 20.2 Error Detection via ISTACK and BSTACK | 285 |
| 20.3 Second Example for Error Detection | 287 |
| 21 The MPI Network | 291 |
| 22 Handling an S7-CPU | 295 |
| 22.1 S7-CPU with Micro Memory Card (MMC) by SIEMENS | 295 |
| 22.1.1 Handling the MMC | 295 |
| 22.1.2 Mode Selector Switch | 296 |
| 22.1.3 General Reset | 296 |
| 22.1.4 Copying RAM to ROM | 297 |
| 22.1.5 Remanence | 297 |
| 22.2 SPEED7 Controllers made by VIPA GmbH | 298 |
| 22.2.1 How to use the MMC Card for VIPA-S7 Controllers | 298 |
| 22.2.2 General Reset with VIPA S7 Controllers | 299 |
| 22.2.3 User memory and Load memory | 299 |
| 22.3 Storage media | 300 |
| 23 Comparator | 301 |
| 23.1 Evaluating Comparison Functions | 302 |
| 23.1.1 Evaluation via Binary Operations | 302 |
| 23.1.2 Evaluating Statusword Bits | 303 |
| 24 Arithmetic Instructions | 304 |

| | |
|--|-----|
| 25 Differences between S5 and S7 | 308 |
| 25.1 Block Types within S5 and S7 | 308 |
| 25.2 Comparison of S5/S7 Instruction Sets | 309 |
| 25.3 Introducing the Variable in S7 | 310 |
| 25.4 Advantages of S7 | 311 |
| 25.5 Further Differences between S5 and S7 | 312 |
| 26 Programming Guidelines within STEP®7 | 314 |
| 27 Indirect Addressing | 321 |
| 27.1 What is “Indirect addressing”? | 321 |
| 27.2 What is a pointer? | 323 |
| 27.3 Memory Indirect Addressing | 325 |
| 27.3.1 Memory Indirect Addressing of Data Types | 327 |
| 27.3.2 Memory Indirect Addressing of Parameter Types | 327 |
| 27.3.3 How to create a Pointer for Indirect Addressing | 329 |
| 27.4 Register Indirect Addressing | 330 |
| 27.5 Indirect addressable Operands | 332 |
| 27.6 Important Notes concerning indirect Programming | 333 |
| 27.6.1 Important notes concerning the use of AR1 register | 333 |
| 27.6.2 Important Note concerning the use of the AR2 Register | 334 |
| 27.7 Using Error-OBs | 335 |
| 27.8 Error Diagnosis within Indirect Addressing | 336 |
| 27.9 Advantages and Disadvantages of Indirect Addressing | 338 |
| 27.10 Golden Rules for Indirect Addressing | 338 |
| 27.11 Further Example for Indirect Addressing | 339 |
| 28 Analog value processing | 349 |
| 28.1 First Example concerning Analog Value Processing | 349 |
| 28.1.1 Developing a PLC Program within WinPLC7 | 350 |
| 28.1.2 Simulating the PLC Program | 353 |
| 28.1.3 Conclusion | 355 |
| 28.2 Second Example concerning Analog Value Processing: Altering an Engine's Number of RPM's | 356 |
| 28.2.1 Creating the PLC Program within WinPLC7 | 356 |
| 28.2.2 Simulation of the PLC Program | 361 |
| 28.2.3 Conclusion | 363 |

| | |
|---|-----|
| 29 CALL ENVIRONMENT | 364 |
| 29.1 Example 1 for the call environment | 364 |
| 29.2 Example 2 for the Call Environment | 367 |
| 29.3 Example 3 for the Call Environment | 369 |
| 30 Hardware Configuration | 372 |
| 30.1 First Example for the Hardware Configuration of an S7-300® | 372 |
| 30.1.1 Selecting the System Family S7-300® and Creating a Rack (Module assembly frame) | 374 |
| 30.1.2 Inserting PS Modules within a Rack | 376 |
| 30.1.3 Placing the CPU module within the rack | 377 |
| 30.1.4 Inserting Digital Input and Output Modules | 378 |
| 30.1.5 Altering the Input and Output Addresses | 381 |
| 30.1.6 Configuration of Analog Inputs | 384 |
| 30.1.7 Configuration of CPU Properties | 385 |
| 30.1.8 Transferring the Configuration to the CPU | 389 |
| 30.1.9 Conclusion of Example 1 concerning Hardware Configuration | 390 |
| 30.2 Second Example for the Configuration of Hardware | 391 |
| 30.2.1 Starting the Hardware Configurator | 392 |
| 30.2.2 Conclusion of Example 2 concerning Hardware Configuration | 399 |
| 31 Configuration of a Profibus DP System | 400 |
| 31.1 Brief Explanation of DP | 400 |
| 31.1.1 Definition of Devices | 400 |
| 31.1.2 Profibus Device Description File (GSD) | 401 |
| 31.1.3 Set-up of Net | 401 |
| 31.2 First Example concerning the Configuration of a Profibus DP | 402 |
| 31.2.1 Configuration of Central Modules | 402 |
| 31.2.2 Linking the DP Interface of the CPU | 405 |
| 31.2.3 Inserting the first DP Slave: ET200X | 408 |
| 31.2.4 Inserting the second DP Slave: ET200S | 411 |
| 31.2.5 Transferring the DP Configuration | 415 |
| 31.2.6 What to be aware of when programming? | 416 |
| 31.3 Example 2 of a Profibus DP Configuration | 417 |
| 31.3.1 Configuration of the Central Station | 417 |
| 31.3.2 Inserting the DP Slave with the DP Address 10: VIPA 253-1DP01 | 422 |
| 31.3.3 Inserting the DP slave with the DP Address 8: Siemens ET200M | 424 |
| 31.3.4 Transferring the Configuration | 428 |

| | |
|---|-----|
| 31.3.5 The PLC Program when using a CP342-DP as the DP Master | 429 |
| 31.3.6 Conclusion of Example 2 of a Profibus DP Configuration | 436 |
| 31.4 Diagnosis within a Profibus DP System | 437 |
| 31.4.1 Example for a Profibus DP System Diagnosis | 437 |
| 31.4.2 Determining the Status of all DP Slaves | 438 |
| 31.4.3 Error Diagnosis of the DP Slave ET200X | 438 |
| 31.4.4 Error Diagnosis of the DP Slave ET200S | 439 |
| 31.4.5 Conclusion | 441 |
| 31.5 Detecting a Breakdown of a DP slave within the PLC Program | 442 |
| 31.5.1 Example for the PLC Program within OB86 | 445 |
| 31.5.2 Conclusion | 446 |
| 32 Configuration of an intelligent DP Slave | 447 |
| 32.1 Example for the Configuration of an intelligent DP Slave (I-Slave) | 447 |
| 32.1.1 Configuration of the DP Master | 447 |
| 32.1.2 Configuration of the I-Slave | 453 |
| 32.1.3 Transmitting the Configurations | 458 |
| 32.1.4 PLC Program within the DP Master | 458 |
| 32.1.5 PLC Program within the I-Slave | 463 |
| 32.1.6 Initial Startup of the DP Master and the I-Slave | 466 |
| 32.1.7 Conclusion | 467 |
| 32.2 Second Example for the Configuration of an Intelligent DP Slave (I-Slave) | 468 |
| 32.2.1 Configuration of the DP Master | 468 |
| 32.2.2 Configuration of the I-Slave | 471 |
| 32.2.3 PLC Program within the DP Master | 472 |
| 32.2.4 PLC Program within the I-Slave | 474 |
| 32.2.5 Initial Startup of the DP Masters and the I-Slave | 476 |
| 32.2.6 Conclusion | 476 |
| 33 Industrial Ethernet | 477 |
| 33.1 Explanation of Terms | 478 |
| 33.2 Configuration of a S7-300® Station with Ethernet CP | 480 |
| 33.2.1 Execution of Programming Device Functions via an Ethernet CP | 484 |
| 33.2.2 Conclusion concerning the Configuration of an S7-300® Station with Ethernet CP | 486 |
| 33.3 Transmission of a Configuration without an MPI Cable | 487 |
| 33.3.1 Conclusion for the Transmission of a Configuration without MPI Cable | 489 |
| 33.4 Exchange of Data between two Stations via Ethernet CPs | 490 |

| | |
|---|------------|
| 33.4.1 Configuration of the First Station | 491 |
| 33.4.2 Configuration of the TCP Connection at the Sender | 492 |
| 33.4.3 Configuration of the Second Station | 496 |
| 33.4.4 Configuration of the TCP Connection on Receiver Side | 498 |
| 33.4.5 PLC Program within Sender | 500 |
| 33.4.6 PLC Program for Receiver | 504 |
| 33.4.7 Initiating the Exchange of Data and Diagnosis of the TCP Connection | 507 |
| 33.4.8 Conclusion | 510 |
| 34 Simplified Configuration of a VIPA SPEED7 | 511 |
| 34.1 Example for the Configuration of a SPEED7 | 512 |
| 34.1.1 Configuration of the local SPEED7 Station | 512 |
| 34.1.2 Configuration of the SPEED7 DP Interface | 518 |
| 34.1.3 Conclusion concerning the Configuration of a SPEED7 | 520 |
| 35 Remote maintenance of S7 controllers | 521 |
| 35.1 Remote Maintenance Access via the Internet to the Ethernet Interface of an S7 Controller | 522 |
| 35.2 Remote Maintenance Access via the Internet to Ethernet Interfaces of multiple S7 Controllers | 525 |
| 35.3 Summary of Remote Access via the Internet to an S7 Controller with an Ethernet Interface | 529 |
| 35.4 Remote Maintenance Access via the Internet and a NetLink-PRO to an S7 Controller | 530 |
| 35.4.1 Accessing multiple connected PLCs via NetLink PRO | 532 |
| 35.4.2 Addressing multiple NetLink PROs via the Internet | 533 |
| 35.4.3 Summary of the Remote Maintenance Access via the Internet and NetLink PRO | 533 |
| 35.5 Remote Maintenance Access via the Telephone Line (Analog or ISDN) | 534 |
| 36 Global data Communication | 536 |
| 36.1 Global Data Table | 537 |
| 36.1.1 Setup of the Global Data Table | 538 |
| 36.2 Example for Global Data Communication | 543 |
| 36.2.1 Starting the Hardware Configurator | 543 |
| 36.2.2 Configuring the first Station | 544 |
| 36.2.3 Configuring the second Station | 548 |
| 36.2.4 Configuring the third Station | 550 |
| 36.2.5 Networking the Hardware of CPUs | 551 |

| | |
|--|------------|
| 36.2.6 Configuration of the Global Data Communication | 552 |
| 36.2.7 Transferring the Configuration Data for the Global Data Communication to the CPUs | 558 |
| 36.2.8 Starting the Global Data Communication | 559 |
| 36.3 Error Detection for Problems within Global Data Communication | 560 |
| 36.3.1 Checking the Status Double Word within the Sender | 560 |
| 36.3.2 Checking the Status Double Word within Receiver | 566 |
| 36.3.3 Conclusion of Error Detection | 568 |
| 36.4 Loading a Global Data Configuration from CPU Stations | 569 |
| 36.4.1 Loading the PLC Stations to the Hardware Configurator | 570 |
| 36.4.2 Call of the Global Data Table | 572 |
| 36.4.3 Compiling the Global Data Table from Configuration Data | 573 |
| 36.4.4 Conclusion | 575 |
| 36.5 Limitations and Principles for Global Data Communication with S7-300® CPUs | 576 |
| 37 Error analysis with the WinPLC-Analyzer | 577 |
| 37.1 Application Area of the WinPLC-Analyzer | 578 |
| 37.2 WinPLC-Analyzer by MHJ-Software | 579 |
| 37.2.1 How to operate the WinPLC-Analyzer by MHJ-Software | 580 |
| 37.3 Accessing a real Controller | 585 |
| 37.4 Evaluating Records | 587 |
| 37.5 Further Information | 587 |
| Appendix | |
| A Overview of S7 and S7 compatible | 588 |
| B Numeral Systems | 611 |
| C Glossary | 616 |
| D Overview of STEP®7 Instructions | 622 |
| E Picture Credits | 647 |
| F Index | 648 |