SIEMENS

Engineering Manual

Medium-voltage converters

Industrial Security

Edition 11/2020

www.siemens.com

SIEMENS

Medium-voltage converters

SINAMICS
Industrial Security

Configuration Manual

Introduction 1

Warranty and liability for application examples 2

Safety instructions 3

Industrial Security 4

General security measures 5

Security measures for SINAMICS medium-voltage converters 6

Additional SINAMICS CU320-x functions A

Service & Support B

References C

11/2020
A5E36912609A

Legal information

Warning notice system

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

⚠ DANGER

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

⚠ WARNING

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

⚠ CAUTION

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

NOTICE

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

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

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

⚠ WARNING

Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

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

Disclaimer of Liability

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

Siemens AG
Large Drives Applications
Vogelweiherstr. 1-15
90441 NÜRNBERG
GERMANY

A5E36912609A
Ⓟ 01/2021 Subject to change

Table of contents

1 Introduction 11

2 Warranty and liability for application examples 13

3 Safety instructions 15

4 Industrial Security 17

4.1 Security information 17

4.2 What is industrial security? 17

4.3 Why is Industrial Security so important? 18
4.3.1 Networking and wireless technology 18
4.3.2 Possible corporate security holes 19

4.4 Security measures in automation and drive technology 20
4.4.1 Security measures 20
4.4.2 Siemens Industrial Holistic Security Concept 21
4.4.3 Standards and regulations 22

4.5 Security management 23

5 General security measures 25

5.1 Overview 25

5.2 Defense in depth concept 25

5.3 Plant safety 26
5.3.1 Physical protection of critical production areas 26

5.4 Network security 27
5.4.1 Network segmentation 28
5.4.1.1 Separation between production and office networks 28
5.4.1.2 Network segmentation with SCALANCE S 28
5.4.2 PROFINET products and SNMP 31
5.4.3 Cloud Security 31

5.5 System integrity 32
5.5.1 System hardening 32
5.5.1.1 Services and ports 32
5.5.1.2 User accounts 32
5.5.1.3 PC/notebooks and mobile devices in an industrial environment 33
5.5.1.4 Data storage 33
5.5.1.5 Transporting data 34
5.5.1.6 Passwords 34
5.5.1.7 Product security notifications 35
5.5.1.8 Virus scanner 35
5.5.1.9 Whitelisting 36
5.5.2 Patch management 36
5.5.2.1 Product software 37
5.5.3 Data integrity 37

5.6 Disposal ... 38

6 Security measures for SINAMICS medium-voltage converters ... 39

6.1 Cabinet security ... 39
6.2 Network security ... 39
6.3 Security measures for the CU320-x Control Unit ... 41
6.3.1 Know-how protection ... 42
6.3.2 Parameters: Access levels + password ... 42
6.3.3 Using the memory card ... 43
6.3.4 Safety Integrated ... 43
6.3.5 Communication services and the CU320-x port numbers used ... 44
6.3.6 Integrated web server ... 47
6.3.7 Information about individual interfaces ... 47
6.3.8 Disposing of the SINAMICS CU320-x ... 48
6.3.9 SINAMICS Startdrive and TIA Portal ... 49
6.3.9.1 SINAMICS Startdrive ... 49
6.3.9.2 SINAMICS STARTER ... 50
6.3.10 SINAMICS Drive Control Chart (DCC) ... 52
6.3.10.1 Industrial security with SINAMICS DCC ... 52
6.3.10.2 Use write and know-how protection ... 55
6.4 Security measures for the industrial PC (IPC) ... 56
6.4.1 Data security ... 56
6.4.2 Windows Security Center ... 57
6.4.3 Updating Windows ... 58
6.4.4 User account ... 59
6.4.4.1 Passwords ... 60
6.4.5 Whitelist ... 60
6.4.6 Certificate setting SINAMICS CU320-x communications ... 61
6.4.7 Updating, backing up and restoring software components ... 61
6.4.7.1 Setting recovery points ... 62
6.4.8 Communication services and the IPC port numbers used ... 62
6.4.9 Deleting IPC data ... 64
6.4.10 Disposing of the IPC ... 64

A Additional SINAMICS CU320-x functions ... 67

A.1 Communication ... 67
A.1.1 Communication according to PROFIdrive ... 67
A.1.1.1 General Information ... 67
A.1.1.2 PROFIdrive application classes ... 70
A.1.1.3 Cyclic communication ... 72
A.1.1.4 Parallel operation of communication interfaces ... 83
A.1.1.5 Acyclic communication ... 86
A.1.1.6 Diagnostics channels ... 98
A.1.1.7 Configuring telegrams in Startdrive ... 107
A.1.2 Communication via PROFIBUS DP ... 109
A.1.2.1 General information about PROFIBUS ... 109
A.1.2.2 Commissioning PROFIBUS ... 115
A.1.2.3 Motion Control with PROFIBUS ... 123
A.1.2.4 Slave-to-slave communication ... 126
A.1.2.5 Messages via diagnostics channels ... 137

A.1.3 Communication via PROFINET IO ... 139
A.1.3.1 General information about PROFINET IO ... 139
A.1.3.2 RT classes for PROFINET IO ... 150
A.1.3.3 PROFINET GSDML ... 155
A.1.3.4 Motion Control with PROFINET ... 157
A.1.3.5 Communication with CBE20 ... 160
A.1.3.6 Communication via PROFINET Gate ... 161
A.1.3.7 PROFINET with 2 controllers ... 165
A.1.3.8 PROFINET media redundancy ... 175
A.1.3.9 PROFINET system redundancy ... 175
A.1.3.10 PROFIenergy ... 178
A.1.3.11 Messages via diagnostics channels ... 185
A.1.3.12 Support of I&M data sets 1...4 ... 187
A.1.4 Communication via Modbus TCP ... 188
A.1.4.1 Configuring Modbus TCP via interface X150 ... 191
A.1.4.2 Configuring Modbus TCP via interface X1400 ... 191
A.1.4.3 Mapping tables ... 192
A.1.4.4 Write and read access using function codes ... 195
A.1.4.5 Communication via data set 47 ... 197
A.1.4.6 Communication procedure ... 202
A.1.4.7 Messages and parameters ... 202
A.1.5 Communication via Ethernet/IP (EIP) ... 203
A.1.5.1 Connecting the drive device to EIP ... 204
A.1.5.2 Requirements for communication ... 205
A.1.5.3 Configuring EIP via the onboard PROFINET X150 interface ... 206
A.1.5.4 Configuring EIP via the X1400 interface at the CBE20 ... 207
A.1.5.5 Supported objects ... 207
A.1.5.6 Integrating the drive device into the EIP network via DHCP ... 218
A.1.5.7 Messages and parameters ... 220
A.1.6 Communication via SINAMICS Link ... 221
A.1.6.1 Basic principles of SINAMICS Link ... 221
A.1.6.2 Configuring and commissioning ... 223
A.1.6.3 Topology ... 227
A.1.6.4 Examples: Transmission times for SINAMICS Link ... 229
A.1.6.5 Communication failure when booting or in cyclic operation ... 229
A.1.6.6 Example ... 230
A.1.6.7 Function diagrams and parameters ... 233
A.1.7 Communication via USS ... 233
A.1.7.1 Basic settings for communication ... 234
A.1.7.2 Telegram structure ... 236
A.1.7.3 Specify user data of telegram ... 237
A.1.7.4 USS parameter channel ... 238
A.1.7.5 USS process data channel (PZD) ... 244
A.1.7.6 Telegram monitoring ... 246
A.1.8 Time synchronization between the control and converter ... 248
A.1.8.1 Setting SINAMICS time synchronization ... 250
A.1.8.2 Messages and parameters ... 251

A.2 Web server ... 252
A.2.1 Fundamentals ... 254
A.2.1.1 Supported Internet browsers ... 254
A.2.1.2 Accessing the web server ... 255
A.2.1.3 Access protection ... 257

A.2.1.4 SINAMICS write and know-how protection ... 259
A.2.1.5 Dialog screen forms in the web server ... 260
A.2.1.6 Changing parameter values ... 261
A.2.1.7 Administrator password ... 262
A.2.1.8 User login ... 264
A.2.1.9 User logout ... 265
A.2.1.10 Layout of the start page ... 266
A.2.1.11 Using SSL/TLS certificates for secure data transfer ... 270
A.2.2 Diagnostic functions ... 297
A.2.2.1 "Drive objects and components" display area ... 297
A.2.2.2 "Alarms" display area ... 299
A.2.2.3 "Diagnostics buffer" display area ... 302
A.2.2.4 "Communication" display area ... 304
A.2.2.5 "Trace files" display area ... 304
A.2.3 Creating and adjusting the parameter list ... 305
A.2.3.1 Overview ... 305
A.2.3.2 Creating a parameter list ... 306
A.2.3.3 Adding parameters ... 307
A.2.3.4 Selecting/entering parameters ... 308
A.2.3.5 Changing the parameter sequence ... 309
A.2.3.6 Deleting parameters ... 309
A.2.3.7 Changing the list properties ... 309
A.2.3.8 Deleting a parameter list ... 309
A.2.4 Backup and restore ... 310
A.2.4.1 Backing up parameters ... 310
A.2.4.2 Restore file parameters ... 311
A.2.4.3 Restoring the factory setting ... 311
A.2.5 System settings ... 312
A.2.5.1 Setting or changing user accounts ... 312
A.2.5.2 Password forgotten ... 314
A.2.5.3 Configuring the IP connection ... 318
A.2.5.4 Using functions that require a license ... 319
A.2.5.5 Updating the firmware via the web server ... 322
A.2.5.6 System restoration ... 326

A.3 Write and know-how protection ... 327
A.3.1 Write protection ... 327
A.3.2 Activating/deactivating write protection ... 328
A.3.3 Know-how protection ... 329
A.3.4 Configuring know-how protection ... 332
A.3.5 Managing the exception list ... 336
A.3.6 Overview of important parameters ... 338

B Service & Support ... 339

C References ... 341

C.1 Additional information ... 341

Index ... 343

Tables

Table A-1 PROFIdrive device classes ... 68

Table A-2 Properties of the Controller, Supervisor and drive units ... 68
Table A-3 Properties of IF1 and IF2 ... 69
Table A-4 Selection of telegrams depending on the PROFIdrive application class ... 70
Table A-5 Properties of the cyclic interfaces IF1 and IF2 ... 84
Table A-6 Implicit assignment of hardware to the cyclic interfaces for p8839[0] = p8839[1] = 99 ... 84
Table A-7 PROFIBUS address switch ... 116
Table A-8 Additional parameters ... 119
Table A-9 Variables: "General" tab ... 120
Table A-10 Time settings and meanings ... 124
Table A-11 Minimum times for reserves ... 125
Table A-12 Comparison between RT and IRT ... 152
Table A-13 Settable send cycles and update cycles ... 154
Table A-14 Submodules depending on the particular drive object ... 156
Table A-15 Time settings and meanings ... 158
Table A-16 Functionality and selection in the pointer file ... 161
Table A-17 Overview of the PROFIenergy measured values ... 183
Table A-18 Parameter designation, assignment and meaning ... 187
Table A-19 Assigning the Modbus register to the parameters - process data ... 192
Table A-20 Assigning the Modbus register to the parameters - parameter data ... 193
Table A-21 Assignment of the Modbus register for general parameter access using DS47 ... 195
Table A-22 Structure of a read request for device number 17, example ... 196
Table A-23 Device response to the read request, example ... 196
Table A-24 Invalid read request ... 196
Table A-25 Write parameter request: Reading parameter value of r0002 from device number 17 ... 199
Table A-26 Start parameter request: Reading parameter value of r0002 from device number 17 ... 199
Table A-27 Response for successful read operation ... 199
Table A-28 Response for unsuccessful read operation - read request still not completed ... 200
Table A-29 Write parameter request: Writing the parameter value of p1121 from device number 17 ... 200
Table A-30 Start parameter request: Writing the parameter value of p1121 from device number 17 ... 200
Table A-31 Response for successful write operation ... 201
Table A-32 Response for unsuccessful write operation - write request still not completed ... 201
Table A-33 Overview of exception codes ... 202
Table A-34 Configurable Control Units and interfaces ... 204
Table A-35 Overview ... 207
Table A-36 Class Attribute ... 208
Table A-37 Instance Attribute ... 208
Table A-38 Explanation for No. 5 of the previous table ... 209
Table A-39 Class Attribute ... 209
Table A-40 Instance Attribute ... 209

Table A-41 Class Attribute 210
Table A-42 Instance Attribute 210
Table A-43 Class Attribute 210
Table A-44 Instance Attribute 211
Table A-45 Class Attribute 212
Table A-46 Instance Attribute 213
Table A-47 Class Attribute 213
Table A-48 Instance Attribute 213
Table A-49 Class Attribute 214
Table A-50 Instance Attribute 214
Table A-51 Class Attribute 216
Table A-52 Class Attribute 217
Table A-53 Compile send data of drive 1 (DO2) 224
Table A-54 Compile send data of drive 2 (DO3) 224
Table A-55 Compile send data of Control Unit 1 (DO1) 225
Table A-56 Receive data for Control Unit 2 226
Table A-57 Corresponding parameters 228
Table A-58 Address switches 234
Table A-59 Request identifiers, control → converter 238
Table A-60 Response identifiers, converter → control 239
Table A-61 Error numbers for response identifier 7 239
Table A-62 Parameter value or connector 241
Table A-63 Offset and page index of the parameter numbers 242
Table A-64 Character runtime 246
Table A-65 Start delay 247

Figures

Figure 4-1 SI HSC security management process 22
Figure 4-2 Security management process 23
Figure 5-1 Defense in depth strategy 25
Figure 5-2 SCALANCE S application example 30
Figure 6-1 Network interfaces (representative diagram only, can vary depending on the specific project) 40
Figure 6-2 Flow of configuration data: TIA-DCC 53
Figure 6-3 Flow of configuration data: Example for DCC Classic V2.1 ... V3.4 (STARTER) 54
Figure 6-4 IPC interfaces 56
Figure A-1 Normalization of speed 75
Figure A-2 Example of encoder interface (encoder 1: Two actual values, encoder 2: One actual value) 77
Figure A-3 Sequence chart for "Find reference mark" 78

Figure A-4 Sequence chart for "Flying measurement" 79
Figure A-5 Overview of "Motion Control with PROFIBUS" (example: controller and 3 devices) 81
Figure A-6 Isochronous drive coupling / motion control with PROFIdrive 82
Figure A-7 Reading and writing data 87
Figure A-8 Task description for multi-parameter request (example) 96
Figure A-9 Components of a message 100
Figure A-10 Example: Telegram configuration with several drive objects 108
Figure A-11 Component and telegram structure 112
Figure A-12 Slave properties – overview 113
Figure A-13 Slave properties – details 114
Figure A-14 Interfaces and diagnostic LED 115
Figure A-15 Monitoring telegram failure with a bus fault 121
Figure A-16 Monitoring telegram failure for a CPU stop 121
Figure A-17 Motion control / isochronous drive coupling with PROFIBUS, optimized cycle with $T_{MAPC} = 2 \cdot T_{DP}$ 123
Figure A-18 Slave-to-slave communication with the publisher-subscriber model 127
Figure A-19 Filter block in the parameterizing telegram (SetPrm) 130
Figure A-20 Example project of a PROFIBUS network in HW Config 131
Figure A-21 Telegram selection for drive object 132
Figure A-22 Detail view of slave configuration 132
Figure A-23 Insert new slot 133
Figure A-24 Configuring the slave-to-slave communication nodes 134
Figure A-25 Slave-to-slave communication - overview 135
Figure A-26 Telegram assignment for slave-to-slave communication 135
Figure A-27 Details after the creation of the slave-to-slave communication link 136
Figure A-28 Activation of PROFIBUS 138
Figure A-29 Bandwidth distribution/reservation, PROFINET IO 141
Figure A-30 RT communication across the limits of synchronization domains 153
Figure A-31 Motion Control / isochronous drive link with PROFINET, optimized cycle with CACF = 2 (Controller Application Cycle Factor) 157
Figure A-32 Schematic representation of SINAMICS PROFINET Gate (in short: PN Gate) 162
Figure A-33 Example, communication sequence 165
Figure A-34 Creating a new S7 project 167
Figure A-35 Automation controller created in HW Config 167
Figure A-36 New project transferred from HW Config into STARTER 168
Figure A-37 Telegram overview for PROFIdrive channel IF1 169
Figure A-38 Add the PROFIsafe telegram to the drive 169
Figure A-39 List of telegrams that are available 169
Figure A-40 The telegrams were aligned with HW Config 170
Figure A-41 Updated project in HW Config 171

Figure A-42 Safety telegrams of the A-CPU enabled 172
Figure A-43 PROFIsafe controller configuration 173
Figure A-44 New project completed in HW Config 174
Figure A-45 New project completed in STARTER 174
Figure A-46 System redundancy with converters 177
Figure A-47 PROFIenergy functions 180
Figure A-48 Energy saving during pauses with PROFIenergy 181
Figure A-49 Activation of PROFINET 186
Figure A-50 Individual components, including Modbus Application Header (MBAP) and function code 195
Figure A-51 Maximum topology 227
Figure A-52 SINAMICS Link: Configuration example 232
Figure A-53 Structure of a USS telegram 236
Figure A-54 USS telegram - user data structure 237
Figure A-55 Telegram for a read request from p7843[2] 241
Figure A-56 Telegram for a read request from p7843[2] 243
Figure A-57 Telegram, to activate the automatic restart with p1210 = 26 243
Figure A-58 Telegram, to assign DI 2 with ON/OFF1 243
Figure A-59 Process data channel 244
Figure A-60 Telegram runtime as the sum of the residual runtime and character delay times 247
Figure A-61 Start delay and response delay 247
Figure A-62 Ping snap 249
Figure A-63 Web server structure 253
Figure A-64 Example of a dialog screen 260
Figure A-65 Example: Display of adjustable parameters 261
Figure A-66 Structure of the web server 266
Figure A-67 Support addresses 269
Figure A-68 Example: Mozilla Firefox 273
Figure A-69 Example: Drive objects display area 297
Figure A-70 Example: “Components” display area 298
Figure A-71 Example: Topology display area 299
Figure A-72 Example: Message list 300
Figure A-73 Example: Further information 300
Figure A-74 Example: Filtering messages 301
Figure A-75 Example: Filtering diagnostic buffers 303
Figure A-76 Example: Communication display area 304
Figure A-77 Prompt to enter the administrator password 317
Figure A-78 Message text when write protection is active 327
Figure A-79 Available protection settings 330
Figure A-80 Exception list with know-how protection password 336

Introduction

1

The "Industrial Security" documentation contains recommendations and information for the planning and design of secure systems or plants. The documentation serves as a reference manual and guideline.

This documentation is only intended as a recommendation. The documentation supports customers in safely operating their controllers or plants. You, as operator, are responsible for implementing the security recommendations.

Validity

The documentation is valid from SINAMICS Runtime SW V5.2. The firmware version is inscribed on the SD card label.

Target group

The documentation is particularly geared toward:

- Planners and project engineers
- IT departments of end users and OEMs

The following knowledge is a prerequisite for implementing the described security concepts:

- Administration of the IT technologies familiar from the office environment
- Configuration of the SINAMICS products used
- Configuration of the products of third-party manufacturers used

Benefits

The "Industrial Security" documentation contains the necessary measures and information for planning and configuring plants and systems. The documentation serves as a reference manual and guideline. This documentation cannot and does not want to suggest that there is 100% security because the current range of threats is much too diverse and complex.

This documentation includes all of the necessary measures that should be taken into account for configuring systems in a secure environment. This documentation is intended to support machine manufacturers (OEMs) in safely operating their controls or system.

Warranty and liability for application examples

2

Application examples are not binding and do not claim to be complete regarding configuration, equipment or any eventuality which may arise. Application examples do not represent specific customer solutions, but are only intended to provide support for typical tasks.

As the user you yourself are responsible for ensuring that the products described are operated correctly. Application examples do not relieve you of your responsibility for safe handling when using, installing, operating and maintaining the equipment.

Note regarding the General Data Protection Regulation

Siemens observes standard data protection principles, in particular the principle of privacy by design. That means that

this product does not process / store any personal data, only technical functional data (e.g. time stamps). If a user links this data with other data (e.g. a shift schedule) or stores personal data on the same storage medium (e.g. hard drive) and thus establishes a link to a person or persons, then the user is responsible for ensuring compliance with the relevant data protection regulations.

Safety instructions

3

Risk of death resulting from failure to observe the safety instructions and residual risks

If you fail to heed and comply with the safety instructions and residual risks in the associated converter documentation, accidents can occur. This can result in severe injury or death.

- Observe the safety instructions in the converter documentation.
- Consider the residual risks in the risk assessment.

Danger as a result of missing or changed parameterization

As a result of incorrect or changed parameterization, machines can malfunction, which in turn can lead to injuries or death.

- Protect the parameterization against unauthorized access.
- Handle possible malfunctions by taking suitable measures, e.g. emergency stop or emergency off.

Unsafe operating states resulting from software manipulation

Manipulation of the software, e.g. viruses, trojans or worms, can result in non-secure operating states in your plant or system. This can result in death, serious injury or material damage.

- Keep the software up to date.
- Incorporate the automation and drive components into a state-of-the-art, integrated Industrial Security concept for the installation or machine.
- Make sure that you include all installed products into the holistic industrial security concept.
- Protect files stored on exchangeable storage media from malicious software by with suitable protection measures, e.g. virus scanners.
- Carefully check all security-related settings once commissioning has been completed.

Industrial Security

4

4.1 Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines, and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions form one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. These systems, machines and components should only be connected to the enterprise network or the Internet if and only to the extent necessary and with appropriate security measures (firewalls and/or network segmentation) in place.

You can find more information on protective measures in the area of industrial security by visiting:
https://www.siemens.com/industrialsecurity.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends performing product updates as soon as they are available and using only the latest product versions. Use of product versions that are no longer supported, and failure to apply latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under
https://www.siemens.com/industrialsecurity.

4.2 What is industrial security?

Definition of industrial security

Generally, industrial security is understood to be all of the measures for protecting against the following:

- Loss of confidentiality due to unauthorized access to data
- Loss of integrity due to data manipulation
- Loss of availability (e.g. due to destruction of data or Denial-of-Service (DoS))

Objectives of industrial security

The objectives of industrial security encompass:

- Fault-free operation and guaranteeing of availability of industrial plants and production processes
- Preventing hazards to people and production due to cyber security attacks

- Protection of industrial communication from espionage and manipulation
- Protection of industrial automation systems and components from unauthorized access and loss of data
- Practicable and cost-effective concept for securing existing systems and devices that do not have their own security functions
- Utilization of existing, open, and proven industrial security standards
- Fulfillment of legal requirements

An optimized and adapted security concept applies for automation and drive technology. The security measures must not hamper or endanger production.

4.3 Why is Industrial Security so important?

4.3.1 Networking and wireless technology

Overview

There are many new trends which affect industrial security:

- Cloud computing in general
  The number of network connections across the world is constantly increasing. This enables innovations such as cloud computing and the applications that go hand in hand with it. In conjunction with cloud computing, there has been a massive increase in the number of mobile devices, such as cell phones and tablet PCs.
- Wireless technology
  On the other hand, the increasing use of mobile devices has only become possible thanks to the ubiquitous availability of mobile networks. Wireless LAN is also becoming increasingly available.
- Worldwide remote access to plants, machines and mobile applications
- The Internet of Things (IoT)
  Millions of electronic devices are becoming network-capable and are communicating via the Internet, such as onboard computers in cars, which transmit warranty information to dealers, or water meter sensors that transmit water consumption data to municipal water suppliers via radio.

However, in order for everything from cloud computing to the Internet of Things to function disturbance-free, you require a reliable network infrastructure and applications that are well protected against attacks from malware and hackers.

4.3.2 Possible corporate security holes

Possible security holes or weak points

The security chain of a company is only as strong as its weakest link. Security holes can exist at numerous points. The following list gives only a few examples:

- Employees / external companies
- Production plants
- Network infrastructure
- Data centers / PC workstations
- Laptops/tablets
- Printers
- Smartphones/smartwatches
- Mobile data storage media

For this reason, a holistic approach is required to deal with the issue of security. Coordinated guidelines and regulations are required that cover all areas: Devices, systems, processes and employees.

The topic of data security and access protection (security) is becoming more and more important in industrial environments. The following technologies results in higher requirements placed on protecting and securing industrial plants and systems:

- The ongoing networking of complete industrial plants and systems
- The vertical integration and networking of various company levels
- New techniques, e.g. remote maintenance and/or remote access

The threats are diverse and the consequences are far-reaching:

Possible threats:

Potential threats come from the industry environment and involve the topic of confidentiality, integrity and availability. Examples of threats include the following:

- Espionage of data, recipes, etc.
- Sabotage of production plants
- System stoppage, e.g. due to virus infection and malware
- Manipulation of data or application software
- Unauthorized use of system functions

Possible effects of a security incident

- Loss of intellectual property
- Loss of production or reduced product quality
- Negative company image and economic damage

- Catastrophic environmental influences
- Danger to people and machines

4.4 Security measures in automation and drive technology

Siemens automation and drive technology concerns itself with security aspects at the following levels:

- **Application security** refers to products and functions that take into consideration the needs of industrial security in the field of automation. This involves particular consideration of the application and task at hand, as well as the people performing the actions in an automated plant. This allows industrial security to be easily implemented in production processes.
- **Security support** provides support during the analysis, planning, implementation, testing and optimization of industrial security - by means of specialists with special knowledge of networks and the industry. These services lead to the highest possible level of industrial security and operating capacity of the production plant.
  Siemens offers comprehensive customer support based on the "Implement Security" service: With this service you can implement protective measures to increase the security level of plants and production facilities. You can find more information about the entire "Implement Security" portfolio on the Internet (https://new.siemens.com/global/en/products/automation/topic-areas/industrial-security/implementation.html).

4.4.1 Security measures

With increasing digitalization, comprehensive security in the automation system is becoming ever more important. For this reason, industrial security is a core element of every product that can be networked.

Integration of security into the products

As manufacturer of automation and drive products, Siemens supports secure operation for its customers by **integrating security into its products**:

- All of the measures involving automation and drive technology are stored in the **Product Lifecycle Management (PLM) process**, which is certified by the German Technical Inspectorate (TÜV) based on IEC 62443-4-1.
- Analytically potential attack threats are detected and evaluated using **Threat and Risk Analyses (TRA)**. Identified critical threats are implemented in the product as necessary basic functions, based on the motto "Security by Design".
- Siemens regularly performs **code analyses** in order to identify and correct possible errors at an early stage during the formal check.

- In its products and its manufacturing process, Siemens has implemented **measures to secure integrity** to indicate any changes to the integrity.
- Siemens constantly checks the measures relating to **hardening**:
  - Operating systems are configured in such a way that **points of attack** (e.g. via ports, unneeded services) are **minimized**.
  - Siemens **tests its products** to detect weak points at an early stage.
  - Siemens offers a focused **hotfix/patch management**service.

Protection of the development infrastructure and supply chain

As manufacturer of automation and drive products, Siemens supports secure operation for its customers by **securing the development infrastructure and supply chain**:

- The Siemens ProductCERT (https://www.siemens.com/cert/en/cert-security-advisories.htm) (**C**yber **E**mergency **R**eadiness **T**eam) is the central department for security-related incidents in the Siemens product and solution environment. Siemens ProductCERT supports development work with consulting and other services. **ProductCERT** provides information about current threats and vulnerabilities as well as the appropriate countermeasures.
- Industrial security is a dynamic and complex subject that requires continuous monitoring and adaptation of new security measures. Information on how Siemens protects its products and solutions against cyber attacks and how industry profits from the competence of Siemens can be found on the Internet (https://new.siemens.com/global/en/products/automation/topic-areas/industrial-security/certification-standards.html).

Provision of patches, security components, and appropriate services

As manufacturer of automation and drive products, Siemens supports secure operation for its customers through direct support of integrators and operating companies **by providing patches, security components and the appropriate services**:

- SIEMENS offers monitoring through a **SIEM system** to monitor residual risk. SIEM stands for Security Information and Event Management and has become an established term in IT security. Such systems are able to identify and evaluate security-relevant events and notify the administrator.
- Additional information is provided here (https://support.industry.siemens.com/cs/ww/en/sc/4992).

4.4.2 Siemens Industrial Holistic Security Concept

Siemens places great emphasis on protecting the integrity and guaranteeing the confidentiality of the processed data for its own products. Intellectual property and know-how of the Siemens products are also in focus.

To achieve this, the Siemens Industrial Holistic Security Concept (SI HSC) is applied which protects development departments and production plants (see the following diagram). Multi-level security systems and basic security improvements of the IT infrastructure are implemented. In parallel, process improvements have been introduced and training in security awareness

provided in the development and production. These measures are being performed continuously by Siemens and clearly demonstrated by the security levels reached.

SI HSC also benefits the customers who Siemens has selected as partners for their industrial solutions, or who want to orientate themselves on the concept. Siemens suppliers are also considered with regard to security so that Siemens already applies the same security standards when purchasing as for the manufacture of its own products.

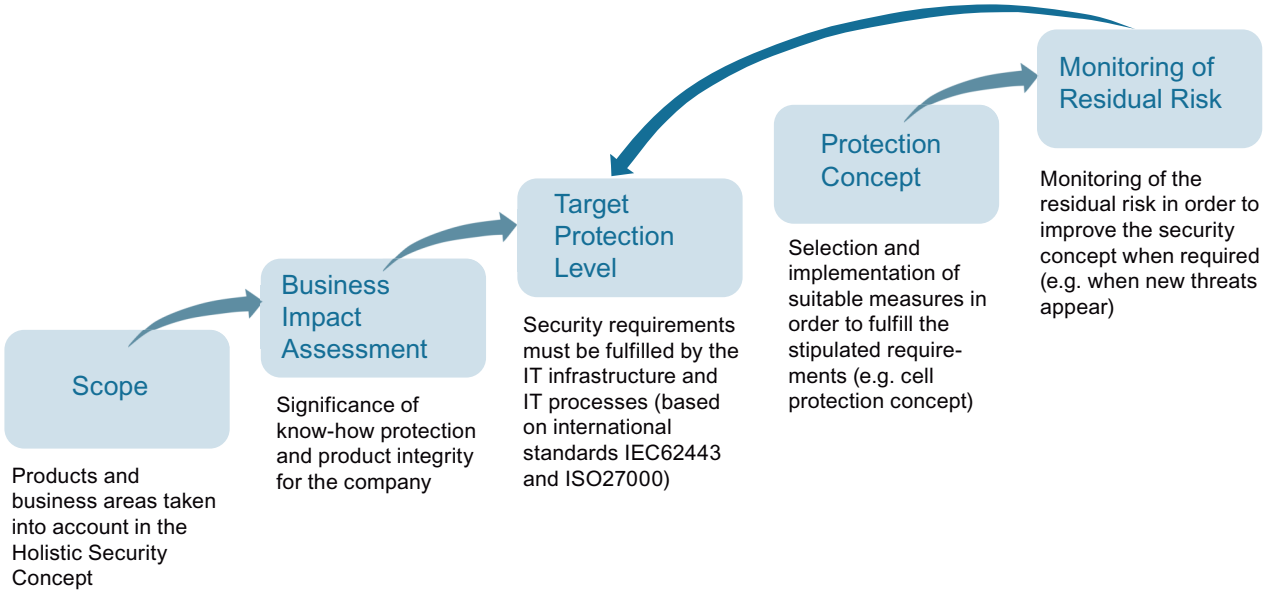


Figure 4-1 SI HSC security management process

Further information

Further information on the Siemens Industrial Holistic Security Concept is available on the Internet on page Always active (https://new.siemens.com/global/en/products/automation/topic-areas/industrial-security/certification-standards.html).

4.4.3 Standards and regulations

Siemens takes the applicable Industrial Security standards and regulations into consideration throughout the entire development process:

- ISO 2700X: Management of information security risks
- IEC 62443: IT security for industrial higher-level control systems – network and system protection

Further information on certifications and standards in the Industrial Security field can be found on the Internet (https://new.siemens.com/global/en/products/automation/topic-areas/industrial-security/certification-standards.html).

4.5 Security management

The security management process as a basis

Protect your system and your company. Security management according to IEC 62443 and ISO 27001 forms the basis for the successful implementation of Industrial Security.

The security management process is shown in the following:

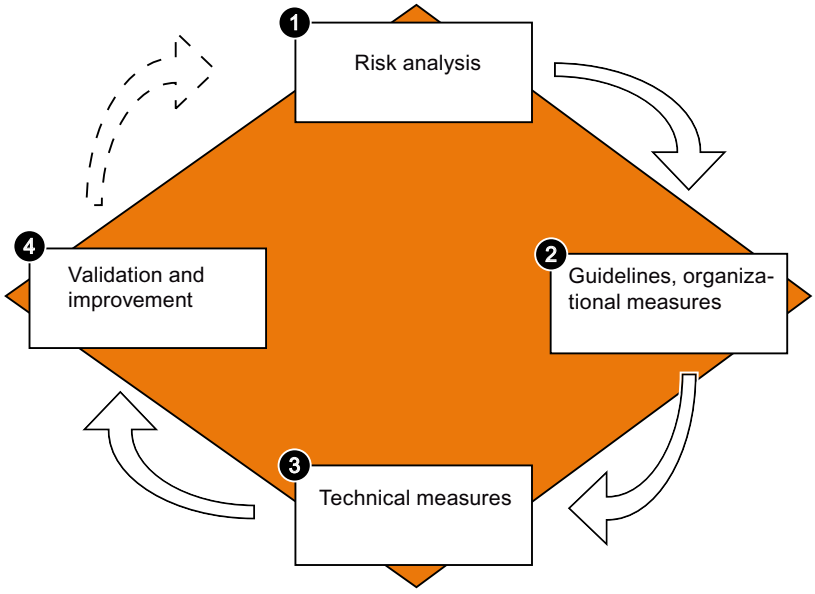


Figure 4-2 Security management process

1. Carry out a risk analysis. Determine all possible risks and define countermeasures for reducing the risk to an acceptable level. In detail, a risk analysis encompasses the following steps:
   - Identification of threatened objects
   - Analysis of value and potential for damage
   - Threat and weak point analysis
   - Identification of existing security measures
   - Risk evaluation
   - Evaluation of the effects with regard to the protection goals relating to confidentiality, integrity and availability
2. Define guidelines and introduce coordinated, organizational measures. To this end, the awareness of the importance of industrial security must be borne by all levels of the company. To achieve a uniform procedure and to support compliance with the defined Industrial Security concept, define the appropriate guidelines and processes.

3. Introduce coordinated technical measures. You can find a list of general measures that help to protect your plant against threats in Section General security measures (Page 25). You can find measures recommended for SINAMICS environments in chapter Security measures for SINAMICS medium-voltage converters (Page 39).
4. A security audit must ensure that all of the measures have been implemented and that they have also eliminated or reduced the identified risks.

Note

Continuous process

Due to constantly changing security threats, this process must be continuously repeated in order to guarantee the security of your plant**.** For this reason, the security management process must be seen as a continuous process.

General security measures

5

5.1 Overview

This chapter describes general security measures that you must take in order to protect your system from threats.

Additional specific security measures for SINAMICS products can be found in chapter "Security measures for SINAMICS (Page 39)".

5.2 Defense in depth concept

To protect industrial plants and systems comprehensively against cyber attacks, measures must be applied simultaneously at all levels. From the operational up to the field level – from access control to copy protection. For this purpose, we use "Defense in Depth" as a general protection concept, according to the recommendations of ISA99 / IEC 62443, the leading standard for security in industrial automation.

Figure 5-1 Defense in depth strategy

Further information on the defense in depth concept and the planning of a protection concept for industrial plants can be found on the Internet (https://new.siemens.com/global/en/products/automation/topic-areas/industrial-security/planning.html).

Protection levels

A defense in depth model has a three level structure:

- **Plant security**
  Plant security represents the outermost protective ring. Plant security includes comprehensive physical security measures, e.g. entry checks, which should be closely coordinated with protective measures for IT security.
- **Network security**
  The measures, grouped under the keyword "Network security", form the core of the protective measures. This refers to the segmentation of the plant network with limited and secure communication between subnetworks ("secure islands") and the interface check with the use of firewalls.
- **System integrity**
  "System integrity" represents the combination of two essential protection aspects. PC-based systems and the control level must be protected against attacks. Steps include the following measures:
  - Integrated access protection mechanisms in the automation components to prevent unauthorized changes via the engineering system or during maintenance
  - The use of antivirus and whitelisting software to protect PC systems against malware
  - Maintenance and update processes to keep the automation systems up-to-date (e.g. patch management, firmware updates, etc.)

5.3 Plant safety

Unauthorized persons may be able to enter the production site/building and damage or alter production equipment as a result of gaps in a company's physical security. Confidential information can also be lost. This can be prevented if both the company's site and the production areas are protected accordingly.

5.3.1 Physical protection of critical production areas

Company security

The company's physical security must be ensured by taking the following measures:

- Closed off and monitored company premises
- Entry control, keys / card readers and/or security personnel

- Escorting of external personnel by company employees
- Security processes in the company are taught and followed by all employees

Physical production security

The physical security of a production location must also be ensured by taking the following measures, for example:

- Separate access control for critical areas, such as production areas
- Installation of critical components in lockable control cabinets / switching rooms including monitoring and alarm signaling options. The control cabinets/contact chambers must be secured by a cylinder lock. Do not use simple locks, such as universal, triangular/square or double-bit locks.
- Configuration of the radio field to restrict the WLAN range so that it is not available outside the defined areas (e.g. factory building).
- Guidelines that prevent the use of third-party data storage media (e.g. USB sticks) and IT devices (e.g. notebooks) classified as insecure on systems.

Additional information

Additional information on integrated Siemens security solutions can be found on the Siveillance page (https://new.siemens.com/global/en/products/buildings/security/security-management.html).

5.4 Network security

Network security includes all measures taken to plan, implement and monitor security in networks. This includes the control of all interfaces, e.g. between the office network and plant network, or remote maintenance access via the Internet.

5.4.1 Network segmentation

5.4.1.1 Separation between production and office networks

One important protective measure for your automation or drive system is the strict separation of the production networks and the other company networks. This separation creates protection zones for your production networks.

Note

The products described in this manual must only be operated in defined protection zones.

Separation by means of a firewall system

In the simplest scenario, separation is achieved by means of an individual firewall system which controls and regulates communication between networks.

See also Network segmentation with SCALANCE S (Page 28)

Separation via a DMZ network

In the more secure variant, the coupling is established via a separate DMZ network. In this case, direct communication between the production network and the company network is completely prevented by firewalls and only takes place indirectly via servers in the DMZ network.

Note

The production networks should also be divided into separate automation cells in order to protect critical communication mechanisms.

General security measures

Observe the general security measures even within protection zones, for example as listed in System hardening (Page 32):

5.4.1.2 Network segmentation with SCALANCE S

Siemens provides SCALANCE S security modules to meet network protection and network segmentation requirements. Further information on SIEMENS SCALANCE S can be found on the Internet (https://siemens.com/scalance-s).

SCALANCE S security module

SCALANCE S security modules with Security Integrated provide:

- Stateful inspection firewall
  In order to implement user-specific control and logging, firewall rules can also be specified that only apply to certain users.
- VPN via IPsec (data encryption and authentication)
  This establishes a secure tunnel between authenticated users whose data cannot be intercepted or manipulated. The most important aspect is the protection against external access via the Internet.
- NAT/NATP (address translation)
- Router functionality (PPPoE, DDNS) for broadband Internet access (DSL, cable)
- SCALANCE S623 with additional VPN port (DMZ) enables the secure connection of an additional network for service and remote maintenance purposes. S623 also permits the secure, redundant connection of subordinate networks by means of routers and firewall redundancy.
- SCALANCE S615 has five Ethernet ports with which different network topologies can be protected by means of a firewall or Virtual Private Network VPN (IPsec and OpenVPN), and security concepts implemented flexibly.

Requirement

NOTICE
Data misuse Long distances between the device to be protected and the upstream security modules represent an invitation for data misuse. • Note that upstream security modules, such as SCALANCE S, must be installed close to the device to be protected in a locked control cabinet. This ensures that data cannot be manipulated here without notice.

Principle

The following application example shows cell segmentation by several SCALANCE S modules, each of which is upstream of the automation cells. The data traffic to and from the devices within automation cells can be filtered and controlled with the SCALANCE S firewall. If required, the traffic between the cells can be encrypted and authenticated. Secure channels and client access from the PCs to the cells can be established via SOFTNET Security Client, VPN client software for PCs.

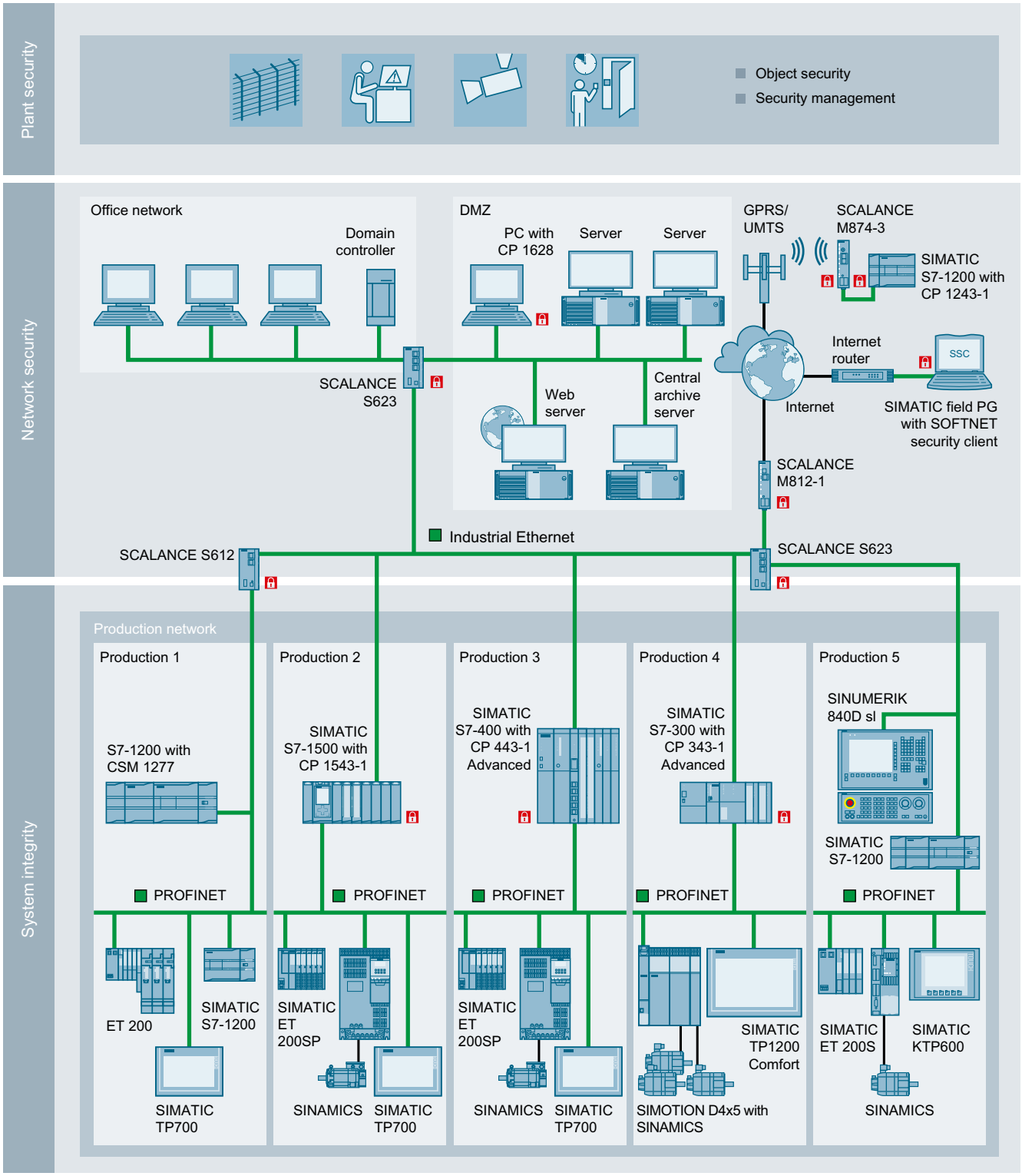


Figure 5-2 SCALANCE S application example

VPN access

Note

Note that a SCALANCE S security module must always be used for VPN access.

5.4.2 PROFINET products and SNMP

Note

Products with PROFINET provide the option of reading out and writing to parameters via **SNMP** (**S**imple **N**etwork **M**anagement **P**rotocol, Port 160/161).

- Do not only identify components based on their SNMP parameters alone, but also use the information provided on the type plate (e.g. MAC address, serial number, etc.).

5.4.3 Cloud Security

Since cloud applications are becoming increasingly common and the cloud continues to grow in its significance, the issue of security in the cloud environment is also becoming more and more important.

The following addresses are designed to give you a general idea of how you can make your system safe in the cloud environment. Inform yourself about the applicable requirements and tried and tested solutions/best practices.

Initial orientation

- Companion Guide for Cloud - CIS Organization (https://www.cisecurity.org/press-release/cis-controls-companion-guide-for-cloud-now-available/)
- Matrix Cloud Control - CSA Organization (https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v3-0-1/)
- Questionnaire Cloud Security - CSA Organization (https://cloudsecurityalliance.org/artifacts/consensus-assessments-initiative-questionnaire-v3-1)
- Top Threats Cloud Security - CSA Organization (https://cloudsecurityalliance.org/research/working-groups/top-threats/)

Siemens Cloud solutions

Siemens offers first-class cloud management paired with excellent know-how for business solutions. This ensures maximum security for our customers. Inform yourself about the Siemens Cloud solutions:

- Industrial Cloud computing (https://www.plm.automation.siemens.com/global/en/our-story/glossary/industrial-cloud-computing/58773)
- Overview of Siemens Cloud portfolio (https://www.sw.siemens.com/portfolio/cloud)
- SIEMENS MindSphere (https://www.plm.automation.siemens.com/global/en/products/mindsphere/)

5.5 System integrity

System integrity

System integrity is understood to mean the "integrity" or "correctness" of the data or the correct response of the system. Thus, the following measures for protecting the system integrity should ensure that the data/functionality of the system cannot be manipulated by unauthorized persons or that manipulations can be detected.

5.5.1 System hardening

5.5.1.1 Services and ports

Activated services and ports represent a risk. To minimize the risk, only the necessary services for all of the automation components should be activated. Ensure that all activated services are taken into account (especially Web servers, FTP, remote maintenance, etc.) in the security concept.

A description of all of the ports used can be found in the Equipment Manuals/Function Manuals of the respective products.

5.5.1.2 User accounts

Any active user account that allows access to the system is thus a potential risk. Therefore, take the following security measures:

- Reduction of configured/activated user accounts to the actually needed minimum
- Use of secure access data for existing accounts. This also involves assigning a secure password.

- Regular checks, especially of the locally configured user accounts
- Regular change of passwords

5.5.1.3 PC/notebooks and mobile devices in an industrial environment

The terminal devices used in industrial environments (PCs, notebooks and mobile devices) must meet the generally applicable security requirements. Therefore, take the following measures:

- The terminal device that is used is set up, administered, regularly checked and patched by the appropriate departments. This ensures it is always kept up-to-date. This also means that software and operating systems which are supported and maintained by the manufacturer are always installed.
- A current virus scanner, which is adapted to the operating system used, must be installed on the terminal device that is used. Both the virus patterns and the software itself must be regularly updated. Or, alternatively, work with the Whitelisting (Page 36) method.
- Activate a firewall with appropriate settings on the terminal device that is used.
- Use a configuration without admin. rights on the terminal device that is used.
- Encrypt all of the hard drives or mass storage units (e.g. eMMC or SSD) of the terminal device that is used to protect sensitive data against unauthorized access.
- Do not use the terminal device for other tasks, e.g. in the office network. This is part of the separation of networks dealt with in Chapter "Separation between production and office networks (Page 28)".
- Secure terminal devices from data theft using a physical lock (e.g. Kensington lock) or do not leave them unmonitored.
- If you leave protected terminal devices at the workstation, always activate the lock mode of the operating system. This prevents access to the terminal device and the contents of the screen can no longer be read.
- Set up user accounts (Page 32) for the access rights accordingly.
- Take appropriate measures to protect unneeded interfaces (e.g. USB, network, etc.) to prevent unauthorized access. This can be done physically using commercially available USB port locks or via corresponding software measures.

5.5.1.4 Data storage

When you store security-relevant data on your PC, you are responsible for secure data storage.

These include, for example, the following measures:

- Consequent marking of your documents according to confidentiality levels by introducing a document classification.
- Protection of your encrypted storage locations, such as sharepoints, against manipulation.

- If absolutely necessary, only store your confidential or security-relevant data encrypted on your PC / systems or the network.
  Security-relevant data includes sensitive data, such as archives, passwords, or executable files (*.exe).
- Regularly back up your security-relevant data and carefully protect it against loss and manipulation.

5.5.1.5 Transporting data

Apply the following measures when transporting data:

- Always encrypt your emails if you send confidential and/or security-relevant data by email.
- If you wish to transport confidential and/or security-relevant data on a data storage medium (USB flash drive, hard disk, etc.), carefully investigate as to which data storage media are considered secure. A regular virus check must be carried out for these data storage media. Always save your data on local data storage media so that the data is encrypted.

These measures are especially important for sensitive data, such as archives, passwords, or executable files (*.exe).

5.5.1.6 Passwords

NOTICE
Data misuse caused by using passwords that are not secure enough Data can be easily misused by using passwords that are not secure enough. Insecure passwords can easily be guessed or decoded. • Therefore, change the default passwords during the commissioning and adapt them at regularly defined intervals. • Also change passwords for functions that you yourself do not use to ensure that such unused functions are not misused. • Always keep your passwords secure, and ensure that only authorized persons have access to these passwords.

Assigning secure passwords

Observe the following rules when creating new passwords:

- When assigning new passwords, make sure that you do not assign passwords that can be guessed, e.g. simple words, key combinations that can be easily guessed, etc.
- Passwords must always contain a combination of upper-case and lower-case letters as well as numbers and special characters. PINS must comprise an arbitrary sequence of digits.
- When assigning a password, always ensure you are adhering to the applicable company specifications, e.g. special password policy of the respective company.

- Observe that, in accordance with the applicable company specifications, passwords with the maximum required minimum length must be assigned.
- Wherever possible and where it is supported by the IT systems, a password must always have a character sequence as complex as possible.

Programs are available that can help you to manage your passwords. Using these programs, you can encrypt, save and manage your passwords and secret numbers – and also create secure passwords.

Additional information on assigning secure passwords can be found in Chapter References (Page 341).

5.5.1.7 Product security notifications

Note

Complying with product security notifications

Threats are extremely diverse in nature and are continually changing. As a consequence, always keep yourself up-to-date on a regular basis through the Industry Online Support (https://support.industry.siemens.com/sc/ww/en/sc/2090) regarding whether there are new and relevant product security notifications for your particular products. Comply with the instructions provided in the product security notifications.

5.5.1.8 Virus scanner

An anti-virus program, virus scanner or virus protection program is a software that can detect, block and, if required, eliminate computer viruses, computer worms or Trojans horses.

In principle, virus scanners can only detect known malware (viruses, worms, Trojans, etc.) or harmful logic and therefore cannot provide protection against all viruses or worms. For this reason, virus scanners can only be considered as a complement to general precautionary measures.

The use of a virus scanner must not impact the production operations of a plant. As the last consequence, this will lead to even a virus-infected computer not being permitted to immediately shut down if this would cause the control of the production process to be lost.

NOTICE

Data misuse when using online virus scanners

If you use an online virus scanner, then security-relevant or confidential data can get into the wrong hands and be misused.

- Therefore, do not check any security-relevant or confidential data via an online virus scanner.

Note

Keep virus scanners up-to-date

Always ensure that the virus scanner database is always up-to-date.

Note

Do not install several virus scanners together.

You must always avoid installing several virus scanners together in one system.

Note

Operation in a local network

Always use a virus scanner when locally connecting with the plant or system network.

5.5.1.9 Whitelisting

The basic philosophy of whitelisting is that all applications are mistrusted, unless they have been classified as trustworthy after an appropriate check. This means that a whitelist is maintained in the system. This whitelist therefore contains all applications that have been classified as trustworthy and consequently can be run on your PC systems.

Whitelisting mechanisms provide additional/alternative protection against undesired applications or malware and unauthorized changes to installed applications or executable files (.exe, .dll).

Heed the corresponding product-specific information (Page 39) to determine whether the use of virus scanners and/or whitelisting is recommended.

5.5.2 Patch management

WSUS

The **WSUS** (Windows Server Update Service) system functionality provided by Microsoft is available for current Windows systems. WSUS supports administrators by providing Microsoft updates in large local networks. WSUS automatically downloads update packages (Microsoft update) from the Internet and offers them to the Windows clients for installation.

The fully automatic update process ensures that Microsoft security updates are always available on Siemens clients.

NOTICE
Security gaps for out-of-date operating systems Note that security updates, hotfixes, etc. are no longer supplied by Microsoft for obsolete operating systems < Windows 10. As a consequence, dangerous security gaps can occur with your operating system. • Therefore always upgrade your operating system - if possible - to the latest version. • If you work with an older operating system, take appropriate additional measures (e.g. whitelisting) to protect your system.

Note

Before installing Microsoft Updates, note the following important points:

- **Prior to the update**, back up the system status for a fallback, if necessary. Ensuring the compatibility of the update with the individual system configuration is the responsibility of the customer.
- Never establish a direct connection to the WSUS server in the Internet! Ensure that the environment is secure and install an intermediate layer (e.g. DMZ network, firewall, SCALANCE S modules, etc.).

5.5.2.1 Product software

Note

Out-of-date product software also represents a potential security gap for attacks.

- As a consequence, always install the latest product software versions.

5.5.3 Data integrity

Data integrity is understood to mean the correctness (integrity) of data and the correct functioning of systems. Ensuring the integrity of the data is thus an essential goal of information security. Integrity protection should not be confused with protecting the confidentiality.

NOTICE

Corruption of data and the resulting malfunctioning of the system

For automation and drive systems as well as controller components, data such as archives and programs can be imported from external sources. This data influences the behavior of these systems and should therefore be protected against unauthorized changes.

Data such as archives, programs, and OA applications can also be saved and archived. The systems currently do not provide the capability of ensuring the integrity of programs, archives, and OA applications.

Therefore take your own measures for ensuring integrity to guarantee the data integrity of your archives, OA applications, or other saved data:

- Apply the Siemens Industrial Holistic Security Concept (Page 20).
- Use digital signatures to protect data.
- Ensure there is sufficient access protection:
  - Restrict access rights such as to data archives/Sharepoints accordingly.
  - Do not send any unencrypted/unsigned emails.

5.6 Disposal

Dispose of the products according to the applicable national regulations. The products described in this manual are extensively recyclable on account of the low-toxic composition of the materials used. To recycle and dispose of your old equipment in an environmentally friendly way, please contact an appropriate disposal company.

Always carefully observe the specific security-related disposal notes:

- Disposing of the SINAMICS CU320-x (Page 48)
- Disposing of the IPC (Page 64)

Security measures for SINAMICS medium-voltage converters

6

The following chapter provides an overview of the security measures for your SINAMICS medium-voltage converter. The chapter describes the measures required to protect your converter from security threats. In addition to ensuring a secure network, you must also comply with the appropriate security measures for the following internal components:

- SINAMICS CU320-x
- SIMATIC IPC for touch panel and SIDRIVE IQ
  Depending on the converter equipping, functions for a touch panel and SIDRIVE IQ are implemented in an IPC (one PC solution) or 2 IPCs.

6.1 Cabinet security

Appropriately secure your SINAMICS converter to prevent damage or manipulation to internal components and to protect your know how. Carefully ensure that the electrical cabinet is installed in an area where access is restricted.

The electrical cabinet can be locked when Option C68 is ordered. This means that only authorized persons can access the components inside the electrical cabinet. Carefully note that the touch panel screen is visible outside the electrical cabinet, and can be read by all persons that pass by.

If the electrical cabinet cannot be locked, carefully ensure that only authorized persons can access the area in which the cabinet is installed.

6.2 Network security

Note

SINAMICS products may only be used in a secure and trusted network. Observe the information on this topic in Chapter "Network segmentation (Page 28)".

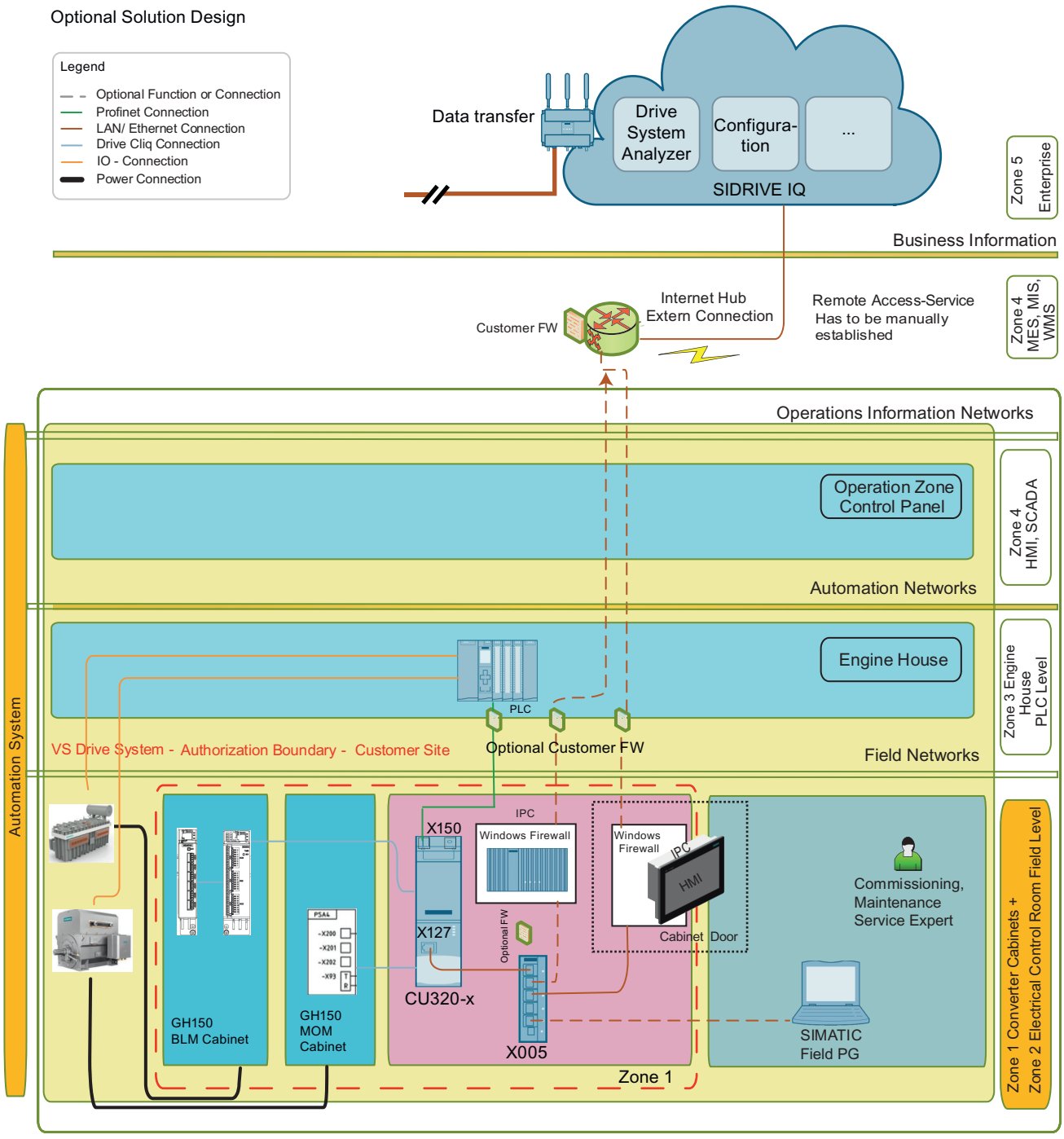


Figure 6-1 Network interfaces (representative diagram only, can vary depending on the specific project)

As shown in the diagram, there are 3 optional network interfaces to the outside of the closed-loop control cabinet that are possible:

- Connecting additional automation components, e.g. PLC, operator panel etc. to the X150 interface of the SINAMICS CU320-x
- Connecting an IPC to SIDRIVE IQ. Depending on the specific version, via the IPC in the operator panel or a separate IPC.
- Connecting an IPC to Remote Access Service (cRSP). Depending on the specific version, via the IPC in the operator panel or a separate IPC.

Securing the network

- Using a firewall, secure the interfaces from the internal network, which are connected with port X127 of the SINAMICS CU320-x. For the IPC, you can use the internal Windows firewall as security measure. You require a separate firewall to establish a connection to the cRSP. To connect additional automation components, we recommend additional security measures according to the overall security concept of your plant/system.
  When configuring your firewall, you must know the ports that are being used. The ports are listed in the appropriate chapter of the "SINAMICS CU320-x (Page 44)" or the "industrial PC (IPC) (Page 62)"
- Carefully secure the control cabinet, so that the internal network cannot be directly accessed. Access for service is an exception to this rule. When carrying out service work, the service technician involved is responsible for security during the time that the controller cabinet is open. The service technician is also responsible for the security of the directly connected SIMATIC Field PG - and where relevant - additional devices for the duration of his work.

6.3 Security measures for the CU320-x Control Unit

An overview of the industrial security features of the SINAMICS CU320-x is provided in this chapter

- Write and know-how protection
- Parameters: Access levels
- Using the memory card
- Note on Safety Integrated
- Communication services and used port numbers
- Web server
- Information about individual interfaces
- SINAMICS Startdrive and STARTER
- SINAMICS Drive Control Chart (DCC)

Detailed descriptions and procedures can be found in the specified SINAMICS documentation (Page 341).

6.3.1 Know-how protection

Some SINAMICS converters provide you with a "Know-how protection" function: This function offers you protection of your intellectual property, especially the know-how of machine manufacturers against unauthorized use, modification or reproduction of their products.

Effect

Adjustable parameters which are not recorded in an exception list can neither be read nor written.

Exceptions

- The know-how protection does not affect parameters that are provided with the following attributes:
  - KHP_WRITE_NO_LOCK
    - These parameters are excepted from the know-how protection and can therefore be written to despite the know-how protection.
    - For a list of these parameters, see the List Manual of the respective product.
    - These parameters are not included in the exception list.
  - KHP_ACTIVE_READ
    - These parameters can also be read, but not written, with activated know-how protection.
    - For a list of these parameters, see the List Manual of the respective product.
    - These parameters are not included in the exception list.
- Know-how protection does not prevent the execution of certain functions:
  - In particular, the "Restore factory settings" function is still possible despite know-how protection.
  - For a full list of executable functions, please refer to the following references.

Additional information

Detailed information on this topic can be found in Appendix:

- Additional functions CU320-x / "Write and know-how protection (Page 327)"
- References (Page 341)

6.3.2 Parameters: Access levels + password

The SINAMICS parameters are divided into access levels 0 to 4. With the aid of the access levels, you can specify which parameters can be modified by which user or input/output device. Parameters of access level 4 are password-protected and only visible for experts.

The converter List Manual specifies in which access level the parameter is displayed and can be changed.

Additional information

You can find detailed information on this topic in chapter "Access protection and rights (Page 257)" and in the List Manual of the converter in chapter "Explanations for the list of parameters".

6.3.3 Using the memory card

The memory card must be handled with particular care for all SINAMICS devices that use a memory card so that no malicious software or erroneous parameterizations are spread between different commissioning PCs or inverters.

WARNING

Risk of death due to software manipulation when using exchangeable storage media

Storing files onto exchangeable storage media amounts to an increased risk of infection of the commissioning PCs, e.g. with viruses or malware. Incorrect parameter assignment can cause machines to malfunction, which can lead to injuries or death.

- Protect files stored on exchangeable storage media from malicious software using appropriate protection measures, e.g. virus scanners.

WARNING

Risk of death due to software manipulation when using exchangeable storage media

Storing the parameterization (incl. Safety Integrated parameterization) on exchangeable storage media carries the risk that the original parameterization (with Safety Integrated) will be overwritten, for example, by the memory card of another drive without Safety Integrated. Incorrect parameter assignment can cause machines to malfunction, which can lead to injuries or death.

- Ensure that only the memory card that belongs to the respective inverter is used.
- Ensure that only trained or authorized personnel have access to the enclosures, cabinets or electrical equipment rooms.

6.3.4 Safety Integrated

To actually reduce the risk for machines and plants through the use of Safety Integrated functions, working with Safety Integrated functions requires special care for all SINAMICS devices that have it.

⚠ DANGER

Unexpected movement of machines caused by inactive safety functions

Inactive or non-adapted safety functions can trigger unexpected machine movements that may result in serious injury or death.

- Observe the information in the appropriate product documentation before commissioning.
- Carry out a safety inspection for functions relevant to safety on the entire system, including all safety-related components.
- Ensure that the safety functions used in your drives and automation tasks are adjusted and activated through appropriate parameterizing.
- Perform a function test.
- Only put your plant into live operation once you have guaranteed that the functions relevant to safety are running correctly.

Note

Important safety notices for Safety Integrated functions

If you want to use Safety Integrated functions, you must observe the safety instructions in the Safety Integrated manuals.

6.3.5 Communication services and the CU320-x port numbers used

When SINAMICS medium-voltage converters are supplied, as standard, the communication protocols listed in the following table are activated at the CU320-x Control Unit.

The following table shows the various layers and protocols that are used.

PROFINET protocols

PROFINET protocols	Port number	(2) Link layer (4) Transport layer	Function	Description
DCP Discovery and Configuration Protocol	Not relevant	(2) Ethernet II and IEEE 802.1Q and Ethertype 0x8892 (PROFINET)	Accessible nodes, PROFINET Discovery and configuration	DCP is used by PROFINET to determine PROFINET devices and to make basic settings. DCP uses the special multicast MAC address: xx-xx-xx-01-0E-CF, xx-xx-xx = Organizationally Unique Identifier
LLDP Link Layer Discovery Protocol	Not relevant	(2) Ethernet II and IEEE 802.1Q and Ethertype 0x88CC (PROFINET)	PROFINET Link Layer Discovery protocol	LLDP is used by PROFINET to determine and manage neighborhood relationships between PROFINET devices. LLDP uses the special multicast MAC address: 01-80-C2-00-00-0E
MRP Media Redundancy Protocol	Not relevant	(2) Ethernet II and IEEE 802.1Q and Ethertype 0x88E3 (PROFINET)	PROFINET medium redundancy	MRP enables the control of redundant routes through a ring topology. MRP uses the special multicast MAC address: xx-xx-xx-01-15-4E, xx-xx-xx = Organizationally Unique Identifier
PTCP Precision Transparent Clock Protocol	Not relevant	(2) Ethernet II and IEEE 802.1Q and Ethertype 0x8892 (PROFINET)	PROFINET send clock and time synchronisation, based on IEEE 1588	PTC enables a time delay measurement between RJ45 ports and therefore the send cycle synchronization and time synchronization. PTCP uses the special multicast MAC address: xx-xx-xx-01-0E-CF, xx-xx-xx = Organizationally Unique Identifier
PROFINET IO data	Not relevant	(2) Ethernet II and IEEE 802.1Q and Ethertype 0x8892 (PROFINET)	PROFINET Cyclic IO data transfer	The PROFINET IO telegrams are used to cyclically transfer IO data between the PROFINET IO controller and IO devices via Ethernet.

PROFINET protocols	Port number	(2) Link layer (4) Transport layer	Function	Description
PROFINET Context Manager	34964	(4) UDP	PROFINET connection less RPC	The PROFINET context manager provides an endpoint mapper in order to establish an application relationship (PROFINET AR).
Network Time Protocol (NTP)	Dynamic	(4) UDP	NTP client; time synchronization	NTP is only supported for onboard PROFINET (X150). An NTP client port (dynamic UDP port > 50000) is only open at this interface.

Connection-oriented communication protocols

Connection-oriented communication protocols	Port number	(2) Link layer (4) Transport layer	Function	Description
ISO on TCP (according to RFC 1006)	102	(4) TCP	ISO-on-TCP protocol	ISO on TCP (according to RFC 1006) is used for the message-oriented data exchange to a remote CPU, WinAC, or devices of other suppliers. Communication with ES, HMI, etc. Is open in the delivery state and is always required.
SNMP Simple Network Management Protocol	161	(4) UDP	Simple network management protocol	SNMP enables the reading out and setting of network management data (SNMP managed Objects) by the SNMP manager. Is open in the delivery state and is always required.
https Secure Hypertext Transfer Protocol	443	(4) TCP	Secure Hypertext transfer protocol	https is used for the communication with the CU-internal web server via Transport Layer Security(TLS). Is open in the delivery state and can be deactivated.
Internal protocol	5188	(4) TCP	Server/ incoming	Communication with commissioning tools for downloading project data.
Reserved	49152...65535	(4) TCP (4) UDP	-	Dynamic port area that is used for the active connection endpoint if the application does not specify the local port.

The complete list of communication services that can be activated, the associated port numbers and detailed information are provided in the Appendix "Communication". (Page 67)

6.3.6 Integrated web server

The web server provides information on a SINAMICS device via its web pages. Access is via an Internet browser. The WEB-HMI also requires access to the web server.

Data transfer

In addition to normal, unsecured HTTP data transfer, the web server also supports secure HTTPS data transfer. Secure HTTPS data transfer is the recommended setting. For security reasons, as default, secure data transfer is forced by deactivating the HTTP port.

Access rights

The normal protection mechanisms of SINAMICS also apply for access via the web server, including password protection. Further protective mechanisms have been implemented especially for the web server. Different access options have been set for different users, depending on the function. The parameter lists are protected so that only users with the appropriate rights can access or change the data.

The administrative web server access is password-protected in the factory. You can access the web server using the following accounts:

- "Administrator" account (full access)
  The "Administrator" account shares the password with the "Administrator" account of the touchscreen operator panel.
- Account "SINAMICS" (restricted access)
  The "SINAMICS" account shares the password with the "Observer" account of the touchscreen operator panel (if a password was assigned).

The initial passwords are provided with the purchase documents. Additional information is provided in Chapter "User Account (Page 59)".

The web interface of the CU320-x should only be directly accessed for maintenance purposes. For converter operation, use the web server integrated in the touchscreen operator panel. For operation, the web server integrated in the touchscreen operator panel requires access to the CU320-x web server.

Additional information

Detailed information on this topic (e.g. Internet browsers that are supported), are listed in the Appendix "Web server (Page 252)".

6.3.7 Information about individual interfaces

X127 LAN (Ethernet)

Ethernet interface X127 is intended for commissioning and diagnostics, which means that it must always be accessible. Note the following restrictions for the X127 interface:

- Only local access is possible
- No networking or only local networking in a locked control cabinet permissible

If you require remote access to the control cabinet, then you must apply additional security measures so that misuse through sabotage, data manipulation by unqualified persons and intercepting confidential data are completely ruled out.

X140 serial interface (RS232)

You connect an external HMI device for operator control/parameter assignment via the serial interface X140.

NOTICE
Access to the inverters only for authorized personnel Unauthorized persons may be able to damage or alter production equipment as a result of gaps in a company's physical security. Confidential information can also be lost or altered as a result of this. You can prevent this if you protect the company site and the production areas accordingly. • You can find information on suitable protective measures in Section "Physical protection of critical production areas (Page 26)".

X150 LAN (Ethernet)

The network with which interface X150 is connected must be separated from the rest of the plant network in accordance with the Defense in Depth concept (see Chapter "General security measures (Page 25)"). Access to cables and possibly open connections must be implemented in a protected fashion, as in a control cabinet.

X1400 LAN (Ethernet)

The network with which interface X1400 is connected must be separated from the rest of the plant network in accordance with the Defense in Depth concept (see Chapter "General security measures (Page 25)"). Access to cables and possibly open connections must be implemented in a protected fashion, as in a control cabinet.

6.3.8 Disposing of the SINAMICS CU320-x

NOTICE
Data misuse resulting from unsafe disposal of the product Unsafe disposal of the product can lead to misuse of the parameter data by third parties. • Before disposal, restore all the parameters to the factory settings.

NOTICE
Data misuse resulting from unsafe disposal of the memory card Unsafe disposal of the memory card can lead to misuse of the data by third parties. For example, data backups required for operating the converter are stored on the memory card. • Clear the memory card before disposing of the product. There are programs that support you in securely deleting/formatting the memory card.

Deleting user-defined certificates

Make sure you securely remove all user-defined certificates before disposing of a SINAMICS product. A hacker can use your certificates to gain access to your protected data transmission.

Delete the files SINAMICS.key and SINAMICS.crt from the directory OEM\SINAMICS\WEB\WEBCONF\CERT on the memory card.

6.3.9 SINAMICS Startdrive and TIA Portal

⚠ WARNING
Malfunctions of the machine as a result of incorrect or changed parameterization As a result of incorrect or changed parameterization, machines can malfunction, which in turn can lead to injuries or death. • Protect the parameter settings against unauthorized access. • Respond to possible malfunctions by applying suitable measures (e.g. EMERGENCY STOP or EMERGENCY OFF).

6.3.9.1 SINAMICS Startdrive

Startdrive in the TIA Portal

SINAMICS Startdrive is an option package in the TIA Portal with which SINAMICS drives are commissioned. With regard to Industrial Security, you must consider the corresponding specifications for SINAMICS drives and for the TIA Portal.

In addition to the commissioning of single drives, you can also use Startdrive to configure drives on SIMATIC control systems such as the S7-1500. Information on how to proceed with SIMATIC controllers can be found in the TIA Portal online help at "Configuring networks".

Commissioning computer

Ensure the security of the commissioning computer. Follow the general security measures (Page 25) for this purpose.

Device know-how protection

- You can protect the parameterization of your drive from unauthorized access via the "know-how protection" function.
- The function is only available online.
- Device know-how protection is supported as of Startdrive V16.

Security functions

- Activation/deactivation of unused functions (web server, ports)
- Write protection for the parameter assignment, p-parameters are readable, but not writeable, protects against unintentional changes to the parameter assignment (only available online).

Protecting backup files in the Windows file system

If you create backup files of charts or projects with Windows tools, also protect these files with Windows tools against unauthorized access using secure passwords. The Startdrive project itself is protected for integrity.

Scripting (Openness)

Scripts (Openness) are used for automating sequences in Startdrive. You must therefore test the scripts before using them on machines.

⚠ WARNING

Risk due to incorrect configurations for automated operating actions

Scripting provides the extensive automation options that are required to be able to automate manual operator actions in the Startdrive tools and therefore to optimize the time required for the recurring configuration of projects and tasks.

The script programmer and the script user are responsible for the operator actions implemented in scripting.

Incorrect configurations that are not discovered in tests can result in serious physical injury or death.

- Run systematic tests on new and modified scripts to verify and validate them.
- Before running a script, make sure it has the correct content. Verify and validate the results of script execution by tests on the machine.

As for DCCs, scripts can also be protected via know-how protection.

6.3.9.2 SINAMICS STARTER

With STARTER, you can put SINAMICS drives into operation.

Commissioning computer

Carefully ensure that the computer used for commissioning is secure. Comply with the general security measures (Page 25).

Protecting backup files in the Windows file system

If you create backup files of diagrams or projects using Windows resources, also protect these files with Windows resources against unauthorized access by using secure passwords.

Security functions

- Know-how protection for the parameter assignment, scripts and DCCs and DCC libraries with password and encryption
- Copy protection for the configuration on the drive unit. The project can only be opened together with the original card.
- Detection of parameter manipulation with STARTER via the project comparison.
- Activation/deactivation of unused functions (web server, ports). For additional information, refer to Section "Web server (Page 252)".
- Write protection for the parameter assignment. p-parameters can be read, but not written. The write protection protects against changes to the parameter assignment and is only available online.

Know-how protection for drive units

In addition to the know-how protection for DCCs, DCC libraries and scripts, you can also protect the parameter assignment of your drive against unauthorized access via the know-how protection for the drive. The function is only available online. You can find information on this in chapter "Write protection and know-how protection (Page 327)".

Scripting

Scripts are used for automated execution in STARTER. You must therefore test the scripts before using them on machines.

⚠ WARNING

Risk due to incorrect configurations for automated operating actions

Thanks to comprehensive automation options, scripting gives you the capability of automating manual operations of the STARTER. As a result, the project and task configuration that is to be repeated is optimized with regard to the time that is spent.

The script programmer and the script user are responsible for the operator actions implemented in scripting.

Incorrect configurations that are not discovered in tests can result in serious physical injury or death.

- Run systematic tests on new and modified scripts to verify and validate them.
- Before running a script, make sure it has the correct content. Verify and validate the results of script execution by tests on the machine.

As for DCC charts, scripts can also be protected via know-how protection.

6.3.10 SINAMICS Drive Control Chart (DCC)

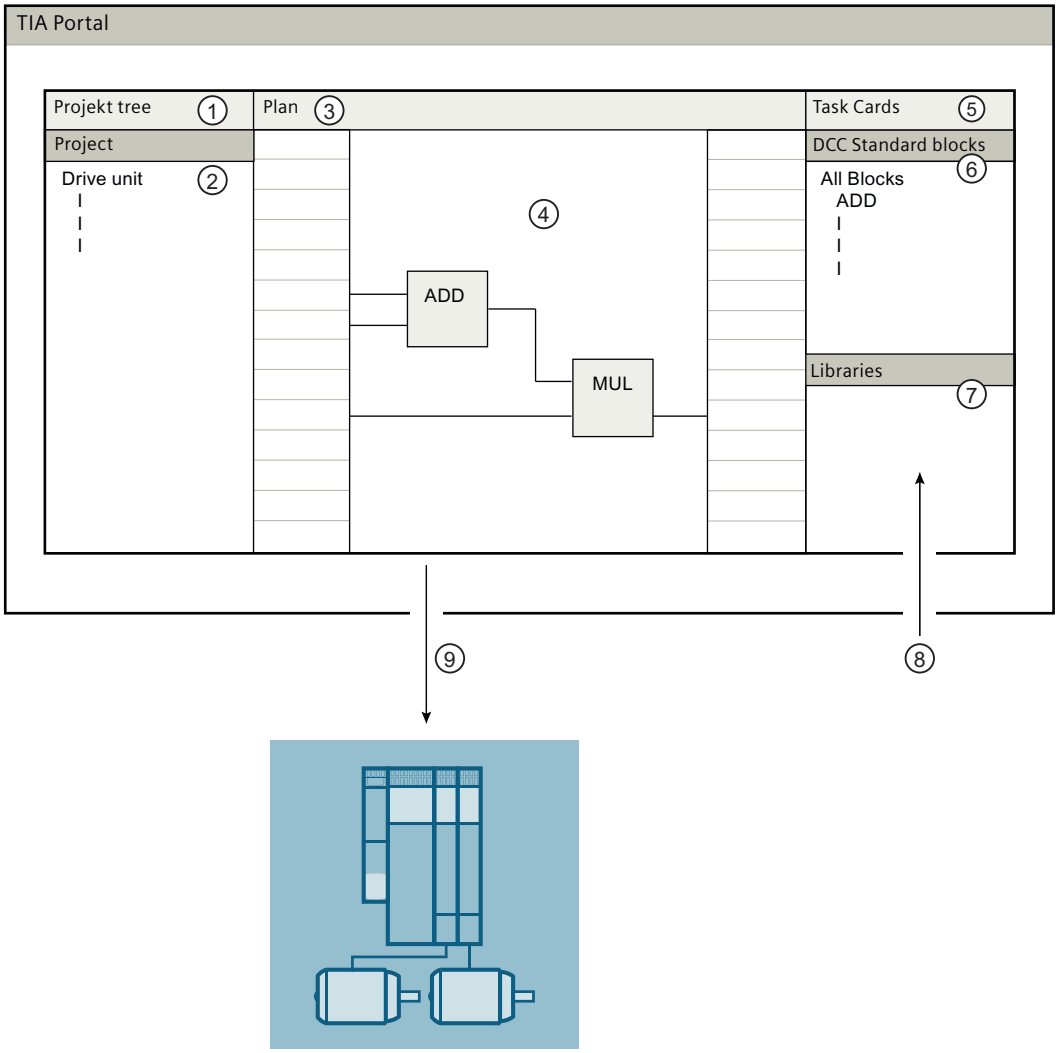
6.3.10.1 Industrial security with SINAMICS DCC

Overview

SINAMICS Drive Control Chart (DCC) offers a modular, scalable technology option, which has chiefly been developed for drive-related, continuous open-loop and closed-loop control engineering tasks within the drive.

With the Drive Control Chart Editor based on CFC, you configure the technology functions with DCC for SINAMICS drives graphically.

- Startdrive
  The following figure shows the data flow of the configuration data when configuring with SINAMICS DCC:



① Loading
② Import of DCB libraries

Figure 6-2 Flow of configuration data: TIA-DCC

- STARTER
  The following figure illustrates the data flow of the configuration data when configuring with SINAMICS DCC and the ways to protect the configured/programmed DCC sources:

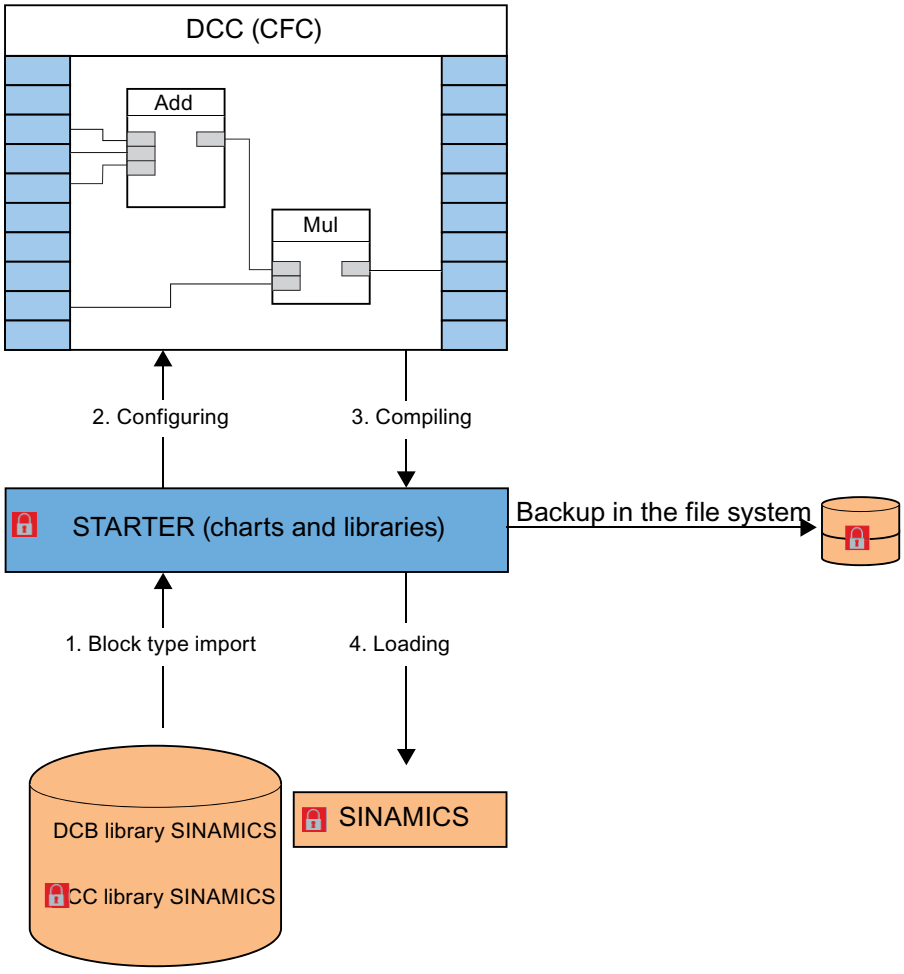


Figure 6-3 Flow of configuration data: Example for DCC Classic V2.1 ... V3.4 (STARTER)

Startdrive: Option package DCC

Note the following special features regarding Startdrive:

- DCC does not provide a backup in the file system.
- The DCB libraries used are loaded implicitly with the project into the target device
- DCC does not offer any chart know-how protection

Commissioning computer

Ensure the security of the commissioning computer. Follow the general security measures (Page 25) for this purpose.

Using know-how protection

DCCs, DCC libraries, programs and backup files are subject to an increased risk of manipulation. Therefore, use the know-how protection, the write protection for drive units and the know-how protection for DCC charts and DCC libraries in STARTER, see also Use write and know-how protection (Page 55).

Information on know-how protection can also be found in the "Motion Control SINAMICS/ SIMOTION Editor Description DCC" Programming and Operating Manual.

Protecting backup files in the Windows file system

If you create backup files of charts or projects with Windows tools, also protect these files with Windows tools against unauthorized access using secure passwords.

Note the information on SINAMICS and on the engineering systems

Also note the Industrial Security information for SINAMICS drives and engineering systems with which SINAMICS drives are commissioned. Particularly the information on network security is important, see also Network security (Page 27).

6.3.10.2 Use write and know-how protection

Prevent unauthorized changes by means of know-how protection

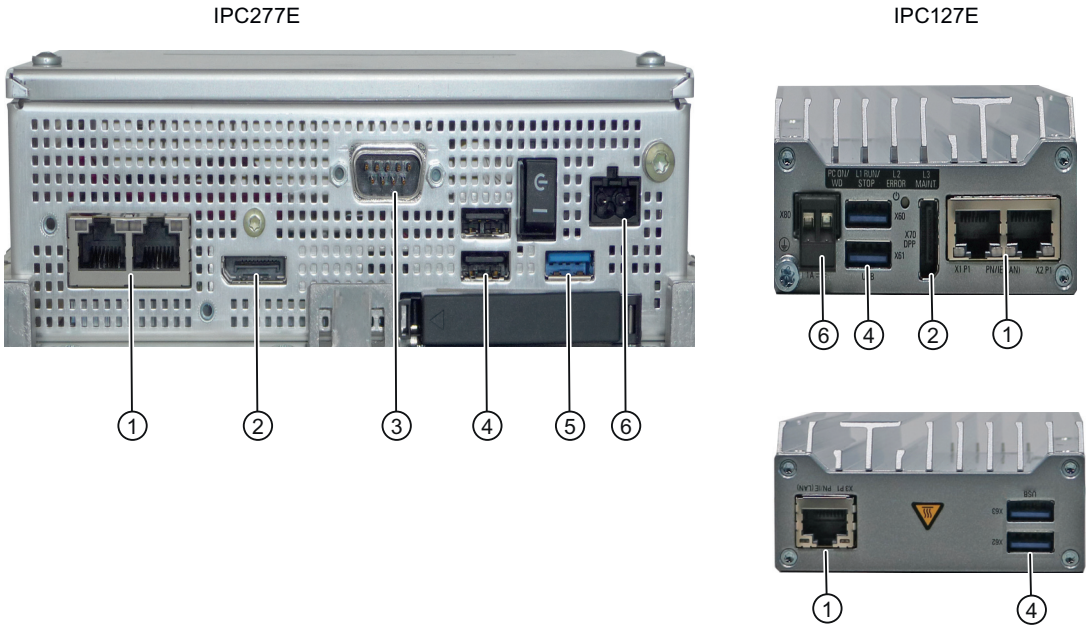
⚠ WARNING

Danger to life through manipulation of DCC charts and DCC libraries

The use of unprotected DCC charts and DCC libraries entails a higher risk of manipulation of DCCs, DCC libraries and backup files.

- Protect important DCC charts and DCC libraries via "Know-how protection programs" or "Know-how protection drive units" in SCOUT or STARTER. Assign a strong password to prevent manipulation.
- Protect important DCC charts and DCC libraries via "Know-how protection drive units" in Startdrive V16 or higher. Assign a strong password to prevent manipulation.
- Therefore, for "Know-how protection programs" or "Know-how protection drive units", use passwords which include at least eight characters, upper and lower case letters, numbers, and special characters.
- Make sure that only authorized personnel can access the passwords.
- Protect the backup files on your file system using a write protection.

6.4 Security measures for the industrial PC (IPC)



①	RJ45 Ethernet ports	②	DisplayPort
③	Serial interface	④	USB-2.0 ports
⑤	USB-3.0 port	⑥	24 V DC power supply

Figure 6-4 IPC interfaces

Protective system of the overall system

The security measures of the touch screen panel, the connectivity module and SIDRIVE IQ applications and the web server do not replace the security system of the overall system itself.

6.4.1 Data security

The IPC saves the converter data unencrypted. Carefully ensure the following:

- Always keep the Windows Firewall activated to protect the device.
- Delete/clear all data from the IPC (Page 64) before returning or disposing of it.
- Regularly backup your security-related data. Information about this is available here. (Page 61)
- Protect the data backup against loss and manipulation.

Hardening measures

Information about hardening measures is available on the Internet (https://www.siemens.com/global/en/home/products/services/cert.html). Under no circumstance weaken the following hardening measures of the connectivity module.

- Verification of the operating system integrity
- Windows updates
- Configuration of the Windows Firewall
- User account control
- Whitelisting

Personal data

The connectivity module neither uses nor processes personal data.

6.4.2 Windows Security Center

The security of your Windows system is ensured by the following safety features:

Standard Windows security features

- Microsoft Defender (Antivirus)
- Windows Firewall
- Windows update

Additionally activated safety features

- Microsoft Windows tool for removing malicious software
- Windows Applocker (whitelisting)
- EMET - Enhanced Mitigation Experience Toolkit

Warning issued by the Windows Security Center

The Windows Security Center issues a warning when you switch on the IPC for the first time. The Security Center checks the status of the device regarding the subsequently listed important security aspects. If a problem has been identified, for example, an out-of-date antivirus software, then the Security Center issues a warning and makes recommendations as to how you can better protect the device.

- **Firewall**: The Windows Firewall helps protect the device by preventing unauthorized users from accessing the device via a network or through the Internet. Windows checks as to whether the device is protected by a software firewall
  The firewall is activated when the device is supplied. Always keep the Windows Firewall activated to protect the device.
- **Antivirus software**: The antivirus software protects the device against viruses and other security threats. Windows checks as to whether comprehensive, topical antivirus software is currently being used on the device.
  The standard Windows antivirus software Microsoft Defender is preinstalled when the device is delivered. Do not install any additional antivirus software.
- **Automatic updates**: Using automatic updates, Windows can routinely search for the latest important updates for the device - which are then automatically installed.
  Additional information is provided in the corresponding IPC Manual, e.g. the touchscreen operator panel
- **Automatic backup:** Using the automatic backup function, Windows can routinely save the files included in the Windows user folders. This option is deactivated when the device is delivered.
- **Realtime protection:** Windows Defender issues a warning if spyware or possibly undesirable software is installed or run on the computer. A warning is also issued if programs attempt to change important Windows settings.

Configure the Security Center corresponding to your requirements.

In addition, the Siemens CERT guidelines (https://www.cert.siemens.com/) are applied to the device.

6.4.3 Updating Windows

NOTICE
Material damage caused a Windows update The IPC must be restarted after a Windows update. As a consequence, the touchscreen operator panel, SIDRIVE IQ etc. functions, which are linked to the IPC, are temporarily not available. This can result in material damage to the system. • If you require functions for safe & secure operation, then the bring the system into a safe & secure state before the Windows update.

Regularly and promptly loading software updates is an important element of a comprehensive security concept. Software updates play an important role in ensuring stable system operation when it comes to closing security gaps that have been identified.

Before carrying out an update, create recovery points for both "C:" and "D:" partitions. Carry out pending Windows updates. You can connect the IPC to the company's own Windows update server.

System update concept

Take into consideration the Windows update topic in the safety concept of your system.

Select the point in time to import the update and to carry out the required restart based on a prior risk assessment. Once a weak point has been identified, carefully assess the situation before deciding on the next steps.

The next steps involve, for example, immediately closing any weak points by installing a security update (if available) or other countermeasures to minimize the risk until the next patch becomes available.

If your risk assessment permits it, you can delay installing the patch until the next possible scheduled plant/system downtime. Define the appropriate steps in advance in your safety concept.

Additional information

Additional information relating to recovery points is provided in Chapter "Setting recovery points (Page 62)" and in the Microsoft Windows Help.

6.4.4 User account

Initial passwords

Together with the purchase documents, you receive initial passwords for the following applications:

- BIOS
- Windows user account ("Admin"/"User")
- Web server passwords ("Administrator"/if required "Observer"/)
- SIDRIVE IQ (when ordered, the password is separately supplied)

Recommendation: Change the initial passwords. Use only strong passwords.

Account authorizations

The operator panel supports 2 different accounts to take into account access security and to improve session management.

- Account "Observer"
- Account "Administrator"

The operator panel display always starts with the Windows user account "Kiosk-User".

If you want to carry out editing work or change Windows settings, then you must switch to the Windows user account "User" or "Admin".

For additional information, refer to the operating instructions of the components in the Appendix References (Page 341).

6.4.4.1 Passwords

Together with the purchase documents, you receive initial passwords for the various accounts. Siemens recommends the following protective measures:

- Change the initial passwords.
- Regularly update the passwords to increase the security level.
- Only use strong passwords. Avoid weak passwords such as "Password1", "123456789".
- Ensure that all passwords are securely protected, and cannot be accessed by unauthorized personnel.
- Do not use the identical password for various accounts.
- Archive your passwords in a secure location that only authorized persons can access. Archive your passwords at several locations.

Note

Losing a password

Access is restricted when a password is lost. The full functionality can only be re-established by replacing the IPC or by reloading the IPC, which involves associated costs. In cases such as these, contact Siemens Service & Support.

6.4.5 Whitelist

The fundamental concept behind what is called a whitelist in the IT domain is that all applications are distrusted. Exceptions are those applications that have been classified as trustworthy after an appropriate check has been made.

A whitelist is maintained and updated in the system. This whitelist includes all applications that have been classified as trustworthy and can be executed on your PC systems.

Whitelisting mechanisms also offer additional protection against the following:

- Undesirable applications and malware
- Unauthorized modifications to installed applications
- Executable files such as .exe, .ps1, .msi.

Do not make any modifications to the whitelist that go beyond commissioning and maintenance activities.

6.4.6 Certificate setting SINAMICS CU320-x communications

The software components of the IPC - e.g. touchscreen panel or SI IQ - communicate with the SINAMICS CU320-x via an HTTPS connection. The HTTPS connection is secured using certificates. In order that the software components of the IPC can access the SINAMICS CU320-x, the web server certificate of the SINAMICS CU320-x must be entered in the certificate memory of the Windows system on the IPC. Only then can the components easily access the SINAMICS CU320-x.

When delivered, the current, automatically generated certificate of the SINAMICS CU320-x is saved in the certificate memory of the Window system on the IPCs. If your converter is equipped with several SINAMICS CU320-x, then the certificate of each SINAMICS CU320-x must be saved in each IPC.

Restoring the trust relating to the web service certificate of the SINAMICS CU320-x

Under certain circumstances, it may be necessary to restore the trust relating to the certificate of the SINAMICS CU320-x web server. To do this, you must again save the certificate of the SINAMICS CU320-x to the certificate memory of the Window system. Reasons for having to change the certificate can include the following, for example:

- An IPC was replaced or added.
- The SINAMICS CU320-x was replaced or had generated a new certificate. Details on this are provided in the Operating Instructions of the SINAMICS CU320-x or in Chapter "Using SSL/TLS certificates for secure data transfer (Page 270)" in Section "Validating a service certificate".
- The certificate has expired.
- You wish to use your own certificate, etc.

Additional information

Additional information, as well as the specific procedure to import the web server certificate of the SINAMICS CU320-x into the IPC, is provided in Chapter "Application scenario Internet Explorer 11 (Page 274)" in Section "Installing the certificate". You must activate the SINAMICS CU320-x web server before importing the certificate.

We recommend that you use your own certificate.

Note

Different configuration of the touchscreen operator panel

Information on how to import the certificate into the IPC of the touchscreen operator panel is provided in the Operating Instructions of the touchscreen operator panel.

6.4.7 Updating, backing up and restoring software components

Recommendation: Before carrying out any maintenance work, create a backup copy of the software components.

Updating the IPC

When required, all updates of software components, e.g. safety-related updates, are provided through Siemens Industry Online Support (https://www.lda-portal.siemens.com/siemlda/en/109773261).

To install software components on the IPC, follow the instructions provided in the Operating Instructions of the corresponding component in Chapter "Activating/deactivating the service mode".

Create a backup copy of the data storage medium for the IPC.

Inserting the connection key (SIDRIVE IQ) after replacing the software image

The following list shows the various application scenarios, and the corresponding measures to insert the connection key:

- Restoring the software image on the IPC with your own backup copy, which was created before commissioning the connectivity module:
  Follow the instructions provided in the Operating Instructions of the connectivity module in Section "Inserting the connection key on the IPC".
- Restoring the software image on the IPC with your own backup copy, which was created after commissioning the connectivity module:
  It is not necessary to reinsert the connection key

Additional information

Additional information on making a backup copy of the data storage medium is provided in the Microsoft Windows Help.

6.4.7.1 Setting recovery points

When switching on the IPC for the first time and before installing any updates, create recovery points for both partitions of the IPC.

Procedure

1. On the IPC desktop, open folder "Troubleshooting".
2. Select script "11_create_recovery_point".
3. In the shortcut menu, execute command "Run as administrator".

6.4.8 Communication services and the IPC port numbers used

When the converter is supplied, as standard, the communication protocols listed in the following table are activated at the IPC.

The activated communication protocols differ depending on the IPC and the software components installed on the IPC. The following table shows the communication protocols depending on the software component.

Connection-oriented communication protocols

Connection-oriented communication protocols	**IPC port number**	**(2) Link layer** **(3) Transport layer** **(4) Transport layer**	**Port number of the communicating partner**	**Description**
X-Tools ports	1394 / 1395	[4] TCP	dynamic (49152...65535)	Ports 1394 / 1395 are open for communication with tool "X-Tools". (only for an IPC with connectivity module)
Remote Desktop Protocol (RDP)	3389	[4] TCP	dynamic (49152...65535)	Using the Remote Desktop Protocol, a Windows session can be remotely established to carry out maintenance work. (only for an IPC with connectivity module)
Hypertext Transfer Protocol (http)	dynamic (49152...65535)	[4] TCP	80	The Windows Update Service requires this for all IPCs with Windows.
Hypertext Transfer Protocol Secure (https)	dynamic (49152...65535)	[4] TCP	443	The Windows Update Service requires this for all IPCs with Windows. This port is also required for the display at the touchscreen operator panel and for the connectivity module to exchange data with the CU320-x. If the IPC is used as cRSP terminal point, when using an SSL tunnel, the port is used for communication with the cRSP server.
ISO on TCP (according to RFC 1006)	dynamic (49152...65535)	[4] TCP	102	ISO on TCP (according to RFC 1006) is used for message-oriented data exchange with CU320-x
Secure Shell (SSH)	22	[4] TCP	dynamic (49152...65535)	Is only opened on an IPC that is used as cRSP terminal point if the tunnel is established via IPsec.
Internet Security Association and Key Management Protocol (ISAKMP)	500/4500	(4) UDP	500/4500	
Encapsulating Security Payload (ESP)	-	[3] ESP (IP protocol number 50)	-	
Authentication Header (AH)	-	[3] AH (IP protocol number 5)	-	

Note

Adapt port

You can individually adapt some ports to address your specific requirements. Create your own list with the individually set ports.

6.4.9 Deleting IPC data

Carefully delete all data on the data storage medium before you return your IPC for repair or you dispose of it. Use the script provided to delete any data on the data storage medium.

Prerequisites

- A Remote Desktop connection has been established from the local service PC to the IPC.
- You have administrator rights

Deleting system-related data using a script

1. Create a backup copy of the data storage medium for the IPC.
2. Activate the service mode.
3. On the IPC desktop, open folder "Troubleshooting".
4. Select script "21_wipe_all_dsc_data_secure".
5. In the shortcut menu, execute command "Run as administrator".
   The operation may take several minutes.

Result

System-related data is reliably deleted according to the NCSC-TG-025 standard of the National Computer Security Center.

6.4.10 Disposing of the IPC

The component can be recycled due to the low level of harmful substances. Contact a company certified for the disposal of electronic waste for environmentally compatible recycling and disposal of your old device. Dispose of the device in accordance with the regulations valid in your country.

If you have any further questions about disposal and recycling, please contact your local Siemens organization.

Procedure

1. Check whether the component is still functional.
2. Delete all data.
3. Dispose of or recycle this component according to the national regulations.

Additional SINAMICS CU320-x functions

A

Note

Extended function description

The following chapters involve an extended function description of the SINAMICS CU320-x. This description is not relevant for security.

Note

SINAMICS converter naming convention

The description in the following Appendices is applicable for many SINAMICS LV and MV converters. Sections and chapters, which make reference to the "SINAMICS S120", are also applicable for your SINAMICS-MV converter.

A.1 Communication

A.1.1 Communication according to PROFIdrive

A.1.1.1 General Information

PROFIdrive is the PROFIBUS and PROFINET profile for drive technology with a wide range of applications in production and process automation systems.

PROFIdrive is independent of the bus system used (PROFIBUS, PROFINET).

Note

PROFIdrive for drive technology is standardized and described in the following document:

- PROFIdrive – Profile Drive Technology,
  PROFIBUS User Organization e. V.
  Haid-und-Neu-Straße 7, D-76131 Karlsruhe,
  Internet: (http://www.profibus.com)
- IEC 61800-7

PROFIdrive device classes

Table A-1 PROFIdrive device classes

PROFIdrive	PROFIBUS DP	PROFINET IO	Example
Peripheral device (P device)	DP slave	IO Device	Drive unit, Control Unit CU320-2
Motion controller (higher-level controller or host of the automation system)	Class 1 DP master	IO Controller	Higher-level control, SIMATIC S7 and SIMOTION
Supervisor (engineering station)	Class 2 DP master	IO Supervisor	Programming devices, human machine interfaces

Note

Consistent naming conventions

For reasons of consistency, the terms "device", "controller", and "supervisor" are used below. The terms "slave" and "master" are only applied in the PROFIBUS chapter and are used there still.

Controller, Supervisor and drive unit

Table A-2 Properties of the Controller, Supervisor and drive units

Properties	Controller	Supervisor	Drive unit
As bus node	Active		Passive
Send messages	Permitted without external request		Only possible on request by the Controller
Receive messages	Possible without any restrictions		Only receive and acknowledge permitted

Communication types

4 communication types are defined in the PROFIdrive profile:

- Cyclic data exchange via a cyclic data channel
  Motion control systems require cyclically updated data in operation for open-loop and closed-loop control tasks. This data must be sent to the drive units in the form of setpoints or transmitted from the drive units in the form of actual values, via the communications system. Transmission of this data is usually time-critical.
- Acyclic data exchange via an acyclic data channel
  The PROFIdrive profile also provides an acyclic parameter channel to exchange parameters between the controller – or the supervisor and drive units. Access to this data is not time-critical.

- Alarm channel
  Alarms are output on an event-driven basis, and show the occurrence and expiry of error states.
- Isochronous mode
  - Cyclic data exchange in a fixed time grid
  - The controller and device are synchronized

Interface IF1 and IF2

The CU320-2 Control Unit can communicate via two different interfaces (IF1 and IF2).

You can assign both interfaces to the following physical interfaces (p8839):

- (1) Onboard X126 PROFIBUS / X150 PROFINET
- (2) Communication Board X1400

Table A-3 Properties of IF1 and IF2

	IF1	IF2
PROFIdrive and SIEMENS telegram	x	-
Free telegram	x	x
Isochronous mode	x	x
Drive object types	All	All
Can be used for	PROFINET IO PROFIBUS DP SINAMICS Link PN Gate Ethernet/IP	PROFINET IO PROFIBUS DP CANopen SINAMICS Link PN Gate Ethernet/IP
Cyclic operation	x	x
PROFIsafe	x	x

Note

For additional information on the IF1 and IF2 interfaces, see Chapter "Parallel operation of communication interfaces (Page 83)" in this manual.

Connecting a PG/PC with the Startdrive commissioning tool

The following connection options are available for Startdrive for commissioning a Control Unit with a PG/PC using a commissioning tool.

- PROFINET
- Ethernet

A.1.1.2 PROFIdrive application classes

There are different application classes for PROFIdrive according to the scope and type of the application processes. PROFIdrive features a total of 6 application classes, the 3 most important are compared here.

- Class 1 (AK1):
  The drive is controlled using a speed setpoint via PROFIBUS/PROFINET. In this case, speed control is fully handled in the drive.
  Typical application examples include simple frequency converters for controlling pumps and fans.
- Class 3 (AK3):
  In addition to the speed control, the drive also includes a positioning control, which means that it operates as an autonomous single-axis positioning drive while the higher-level technological processes are performed in the control system. Positioning requests are transferred to the drive controller via PROFINET (or PROFIBUS) and started.
- Class 4 (AK4):
  This PROFIdrive application class defines a speed setpoint interface, where the speed control is realized in the drive and the closed-loop position control in the control system, such as is required for robotics and machine tool applications with coordinated motion sequences on multiple drives.
  Motion control is primarily implemented using a central numerical controller (NC). The position control loop is closed via the bus, i.e. the communication between the controller and the drive must be isochronous.

Selection of telegrams depending on the PROFIdrive application class

The following Table provides an overview of which telegram can be used reach which PROFIdrive application class:

Table A-4 Selection of telegrams depending on the PROFIdrive application class

Telegram (p0922 = x)	Description	Class 1	Class 3	Class 4
1	Speed setpoint, 16-bit	x	-	-
2	Speed setpoint, 32-bit	x	-	-
3	Speed setpoint, 32-bit with 1 position encoder	x	-	x
4	Speed setpoint, 32-bit with 2 position encoders	x	-	x
5	Speed setpoint, 32 bit with 1 position encoder and Dynamic Servo Control	-	-	x
6	Speed setpoint, 32 bit with 2 position encoders and Dynamic Servo Control	-	-	x
7	Basic positioner with selection of the traversing block	-	x	-
9	Basic positioner with direct setpoint input (MDI)	-	x	-
20	16-bit speed setpoint for VIK-Namur	x	-	-
81	Standard encoder	-	-	-
82	Standard encoder with speed actual value 16 bit	-	-	-
83	Standard encoder with speed actual value 32 bit	-	-	-
102	Speed setpoint, 32 bit with 1 position encoder and torque reduction	x	-	x

Telegram (p0922 = x)	Description	Class 1	Class 3	Class 4
103	Speed setpoint, 32 bit with 2 position encoders and torque reduction	x	-	x
105	Speed setpoint, 32 bit with 1 position encoder, torque reduction and Dynamic Servo Control	-	-	x
106	Speed setpoint, 32 bit with 2 position encoders, torque reduction and Dynamic Servo Control	-	-	x
110	Basic positioner with direct setpoint input (MDI), override and position actual value	-	x	-
111	Basic positioner with direct setpoint input (MDI), override, position actual value and speed actual value	-	x	-
116	32-bit speed setpoint with 2 position encoders, torque reduction, DSC and additional actual values	-	-	x
118	32-bit speed setpoint with 2 position encoders, torque reduction, DSC, additional actual values and 2 external encoders	-	-	x
125	Dynamic Servo Control with torque precontrol, 1 position encoder (encoder 1)	-	-	x
126	Dynamic Servo Control with torque precontrol, 2 position encoders (encoder 1 and encoder 2)	-	-	x
136	Dynamic Servo Control with torque precontrol, 2 position encoders (encoder 1 and encoder 2), 4 trace signals	-	-	x
138	Dynamic Servo Control with torque precontrol, 2 external position encoders (encoder 2 and encoder 3), 4 trace signals	-	-	x
139	Speed/position control with Dynamic Servo Control and torque precontrol, 1 position encoder, clamping status, additional actual values	-	-	x
146	Closed-loop speed/position control with Dynamic Servo Control and torque precontrol, 2 position encoders (encoder 1 and encoder 2), additional actual values, adaptation parameters	-	-	x
148	Closed-loop speed/position control with Dynamic Servo Control and torque precontrol, 2 external position encoders (encoder 2 and encoder 3), additional actual values, adaptation parameters	-	-	x
149	Speed/position control with Dynamic Servo Control and torque precontrol, 1 position encoder, clamping status, additional actual values, adaptation parameters	-	-	x
166	Hydraulic axis (HLA) with two encoder channels and HLA additional signals	-	-	-
220	Speed setpoint, 32 bit, metal industry	x	-	-
352	16-bit speed setpoint for PCS7	x	-	-
370	Infeed	-	-	-
371	Infeed, metal industry	-	-	-
390	Control Unit with digital inputs DI 0 ... DI 15 and digital outputs DO 8 ... DO 15	-	-	-
391	Control Unit with digital inputs DI 0 ... DI 15, DO 8 ... DO 15 and 2 probes	-	-	-
392	Control Unit with digital inputs DI 0 ... DI 15, digital outputs DO 8 ... DO 15 and 6 probes	-	-	-

Telegram (p0922 = x)	Description	Class 1	Class 3	Class 4
393	Control Unit with digital inputs DI 0 ... DI 22, digital outputs DO 8 ... DO 16, 8 probes and analog input	-	-	-
394	Control Unit with digital inputs DI 0 ... DI 22 and digital outputs DO 8 ... DO 16	-	-	-
395	Control Unit with digital inputs DI 0 ... DI 22, digital outputs DO 8 ... DO 16 and 16 probes	-	-	-
700	Supplementary PZD-0/3	-	-	-
701	Supplementary PZD-2/5	-	-	-
750	Supplementary PZD-3/1	-	-	-
999	Free interconnection and length	x	x	x

Dynamic Servo Control (DSC)

The PROFIdrive profile contains the "Dynamic Servo Control" control concept. This requires PROFIdrive application class 4 and transfers not only the speed setpoint, but also the KPC position controller gain factor and the XERR system deviation. With the aid of this data, the position controller can be calculated in the drive. The position setpoint interpolation is still performed in the controller. This can be used to significantly increase the dynamic stability/ stiffness of the position control loop in PROFIdrive application class 4.

A.1.1.3 Cyclic communication

Cyclic communication is used to exchange time-critical process data (e.g. setpoints and actual values).

The process data (PZD) that is to be transferred is defined through the configuration of the drive unit (Control Unit). From the perspective of the drive unit, the received process data represents the receive words and the process data to be sent the send words.

PROFIdrive telegrams

- Standard telegrams
  The standard telegrams are structured in accordance with the PROFIdrive profile. The drive-internal process data links are set up automatically in accordance with the set telegram number.
  The SINAMICS S120/S150 List Manual contains the standard telegrams in the following function diagrams:
  - 2415 PROFIdrive - Standard telegrams and process data 1
  - 2416 PROFIdrive - Standard telegrams and process data 2
- Manufacturer-specific telegrams
  The manufacturer-specific telegrams are structured in accordance with internal company specifications. The drive-internal process data links are set up automatically in accordance with the set telegram number.
  The SINAMICS S120/S150 List Manual contains the manufacturer-specific telegrams (SIEMENS telegrams) in the following function diagrams:
  - 2419 PROFIdrive - Manufacturer-specific telegrams and process data 1
  - 2420 PROFIdrive - Manufacturer-specific telegrams and process data 2
  - 2421 PROFIdrive - Manufacturer-specific telegrams and process data 3
  - 2422 PROFIdrive - Manufacturer-specific telegrams and process data 4
- Supplementary telegrams
  The SINAMICS S120/S150 List Manual contains supplementary telegrams in the following function diagrams:
  - 2423 PROFIdrive - Manufacturer-specific/free telegrams and process data
- Free telegrams (p0922 = 999)
  The SINAMICS S120/S150 List Manual contains free telegrams in the following function diagrams:
  - 2468 PROFIdrive – IF1 receive telegram, free interconnection via BICO (p0922 = 999)
  - 2470 PROFIdrive – IF1 send telegram, free interconnection via BICO (p0922 = 999)

  The receive and send data can be freely connected using BICO technology.

Process data

	SERVO, TM41	VECTOR	CU_S	A_INF, B_INF, S_INF	TB30, TM31, TM15DI_DO, TM120, TM150	ENCODER
Receive process data						
DWORD connector output	r2060[0 ... 18]	r2060[0 ... 30]	-	-	-	r2060[0 ... 2]
WORD connector output	r2050[0 ... 19]	r2050[0 ... 31]	r2050[0 ... 19]	r2050[0 ... 9]	r2050[0 ... 4]	r2050[0 ... 3]

	SERVO, TM41	VECTOR	CU_S	A_INF, B_INF, S_INF	TB30, TM31, TM15DI_DO, TM120, TM150	ENCODER
Binector output	r2090.0 ... 15 r2091.0 ... 15 r2092.0 ... 15 r2093.0 ... 15			r2090.0 ... 15 r2091.0 ... 15		r2090.0 ... 15 r2091.0 ... 15 r2092.0 ... 15 r2093.0 ... 15
Free connector-binector converter	p2099[0 ... 1] / r2094.0 ... 15, r2095.0 ... 15					
Send process data						
DWORD connector input	p2061[0 ... 26]	p2061[0 ... 30]	-	-	-	p2061[0 ... 10]
WORD connector input	p2051[0 ... 27]	p2051[0 ... 31]	p2051[0 ... 24]	p2051[0 ... 9]	p2051[0 ... 4]	p2051[0 ... 11]
Free binector-connector converter	p2080[0 ... 15], p2081[0 ... 15], p2082[0 ... 15], p2083[0 ... 15], p2084[0...15] / r2089[0 ... 4]					

Telegram interconnections

- The telegram interconnection is made automatically and blocked.
  Telegrams 20, 111, 220, 352 are exceptions. There, in addition to the fixed interconnections, selected process data (PZD) can be interconnected as required in the send/receive telegram.
- When you change p0922 ≠ 999 to p0922 = 999, the previous telegram interconnection is retained. You can now change this telegram interconnection.
- If p0922 = 999, a telegram can be selected in p2079. A telegram interconnection is automatically made and blocked. The telegram can also be extended.
  This is an easy method for creating extended telegram interconnections on the basis of existing telegrams.

The telegram structure

- Parameter p0978 contains the drive objects that use a cyclic PZD exchange. All drive objects after the first zero do not participate in the cyclic exchange.
- If the value 255 is written to p0978, this drive object is visible to the PROFIdrive controller and empty (without actual process data exchange). This permits cyclic communication of a PROFIdrive controller in the following cases:
  - with unchanged configuration to drive units that have a different number of drive objects.
  - with deactivated drive objects, without having to change the project
- One PZD = one word.

- Physical word and double word values are inserted in the telegram as referenced variables.
- p200x apply as reference variables (telegram contents = 4000 hex or 4000 0000 hex in the case of double words if the input variable has the value p200x).

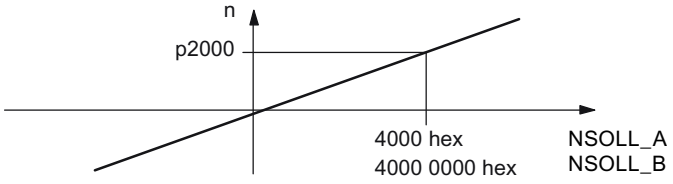


Figure A-1 Normalization of speed

You can find the detailed structure of the telegrams in the SINAMICS S120/S150 List Manual in the associated function diagrams.

Which drive objects support which telegrams?

Drive object	Telegrams (p0922)	Function diagrams
A_INF	370, 371, 999	2421, 2423
B_INF	370, 371, 999	2421, 2423
S_INF	370, 371, 999	2421, 2423
SERVO	1, 2, 3, 4, 5, 6, 102, 103, 105, 106, 116, 118, 125, 126, 136, 138, 139, 146, 148, 149, 220, 999	2415, 2419, 2420, 2423
SERVO (EPOS)	7, 9, 110, 111, 999	2415, 2423
SERVO (position control)	139, 149, 999	2420, 2423
VECTOR	1, 2, 3, 4, 20, 220, 352, 999	2415, 2416, 2421, 2423
VECTOR (EPOS)	7, 9, 110, 111, 999	2415, 2419, 2423
ENC	81, 82, 83, 999	2416, 2423
TM15DI_DO	No predefined telegram.	-
HLA	166, 999	2415, 2420, 2423
TM31	No predefined telegram.	-
TM41	3, 999	2415, 2423
TM120	No predefined telegram.	-
TM150	No predefined telegram.	-
TB30	No predefined telegram.	-
CU_S	390, 391, 392, 393, 394, 395, 999	2422, 2423

Number of process data per drive object

Depending on the drive object, different process data (PZD) can be sent and received:

Drive objects	Maximum number of PZD	
	Send	**Receive**
A_INF	10	10
B_INF	10	10
S_INF	10	10
SERVO	28	20
VECTOR	32	32
ENC	12	4
TM15DI_DO	5	5
TM31	5	5
TM41	28	20
TM120	5	5
TM150	5	5
TB30	5	5
CU	25	20

Interface Mode

Interface Mode is used for displaying the assignment of the control and status words in line with other drive systems and standardized interfaces.

Interface Mode cannot be set by p2038, but rather by setting the telegrams in p0922:

- When standard telegram 20 is set, the "VIK-NAMUR" Interface Mode is permanently specified (p2038 = 2). This relationship cannot be changed.
- When telegrams 102, 103, 105, 106, 116, 118, 125, 126, 136, 138, 139, 146, 148, 149 and 166 are set, the "SIMODRIVE 611 universal" Interface Mode is permanently specified (p2038 = 1). This relationship cannot be changed.
- When all other telegrams are set, the "SINAMICS" Interface Mode is permanently specified (p2038 = 0). This relationship cannot be changed.

Information about control words and status words

Overview of control words and setpoints

A detailed overview of the control words and setpoints is contained in the SINAMICS S120/S150 List Manual in the following function diagrams:

- 2439 PROFIdrive - PZD receive signals, profile-specific interconnection
- 2440 PROFIdrive - PZD receive signals, manufacturer-specific interconnection

Overview of status words and actual values

A detailed overview of the status words and actual values is contained in the SINAMICS S120/ S150 List Manual in the following function diagrams:

- 2449 PROFIdrive - PZD send signals, profile-specific interconnection
- 2450 PROFIdrive - PZD send signals, manufacturer-specific interconnection

Examples

Based on the PROFIdrive communication of the encoder interface, the following application examples show:

- The chronological sequence of the communication
- The chronological changes to the control and status words
- The mutual dependencies of these changes

Examples:

- Example: Encoder interface (Page 77)
- Example: Find reference mark (Page 77)
- Example: Flying measurement (Page 78)

Example: Encoder interface

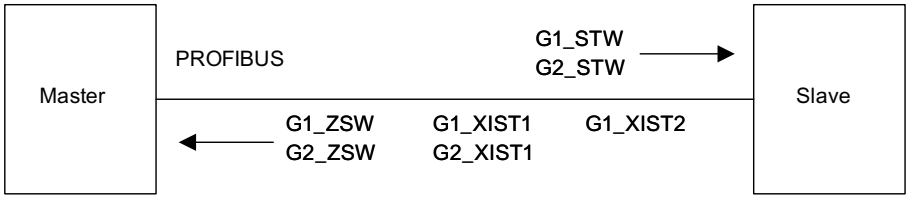


Figure A-2 Example of encoder interface (encoder 1: Two actual values, encoder 2: One actual value)

Example: Find reference mark

Assumptions for the example:

- Distance-coded reference mark
- Two reference marks (function 1 / function 2)
- Position control with encoder 1

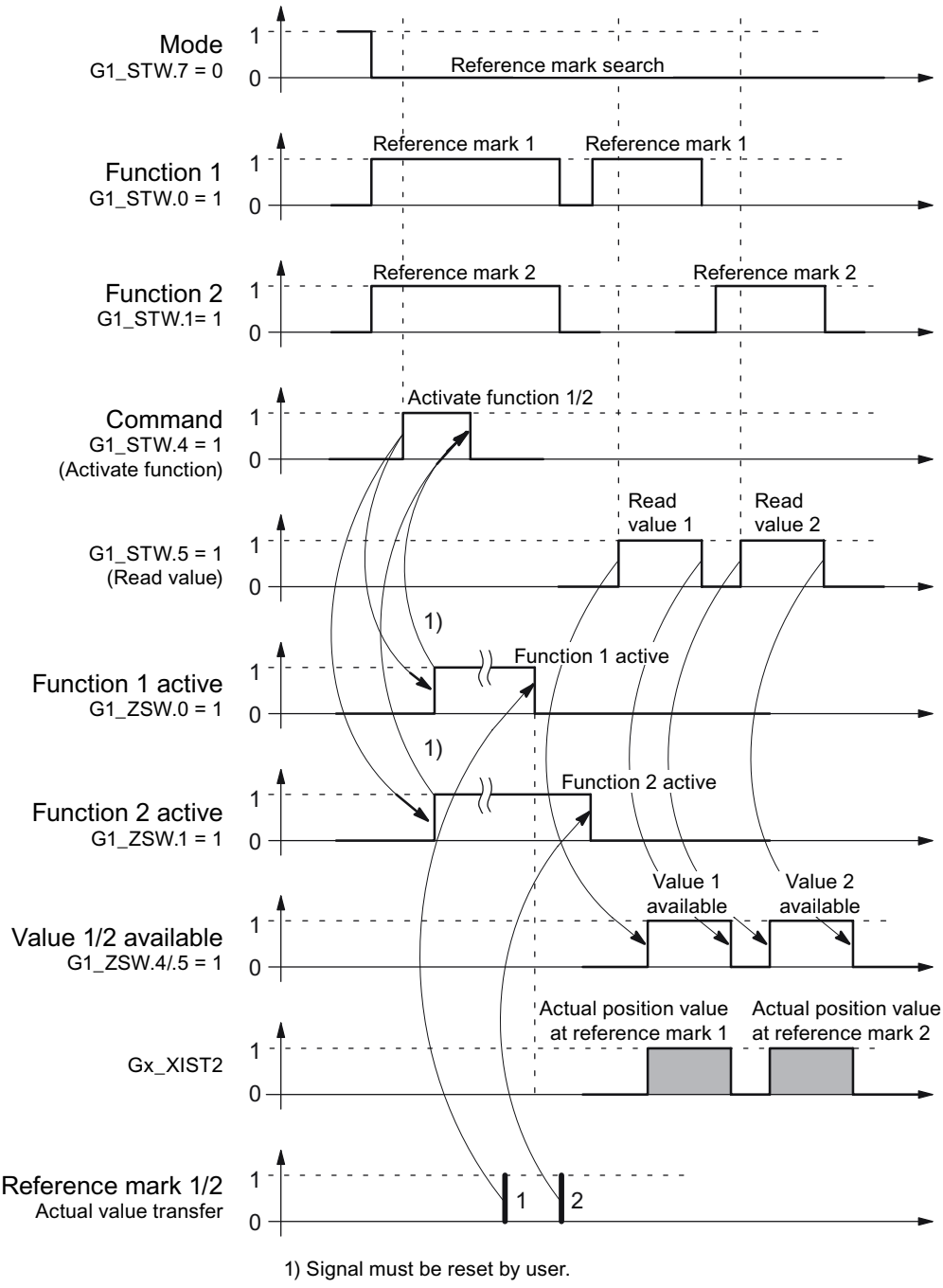


Figure A-3 Sequence chart for "Find reference mark"

Example: Flying measurement

Assumptions for the example:

- Measuring probe with rising edge (function 1)
- Position control with encoder 1

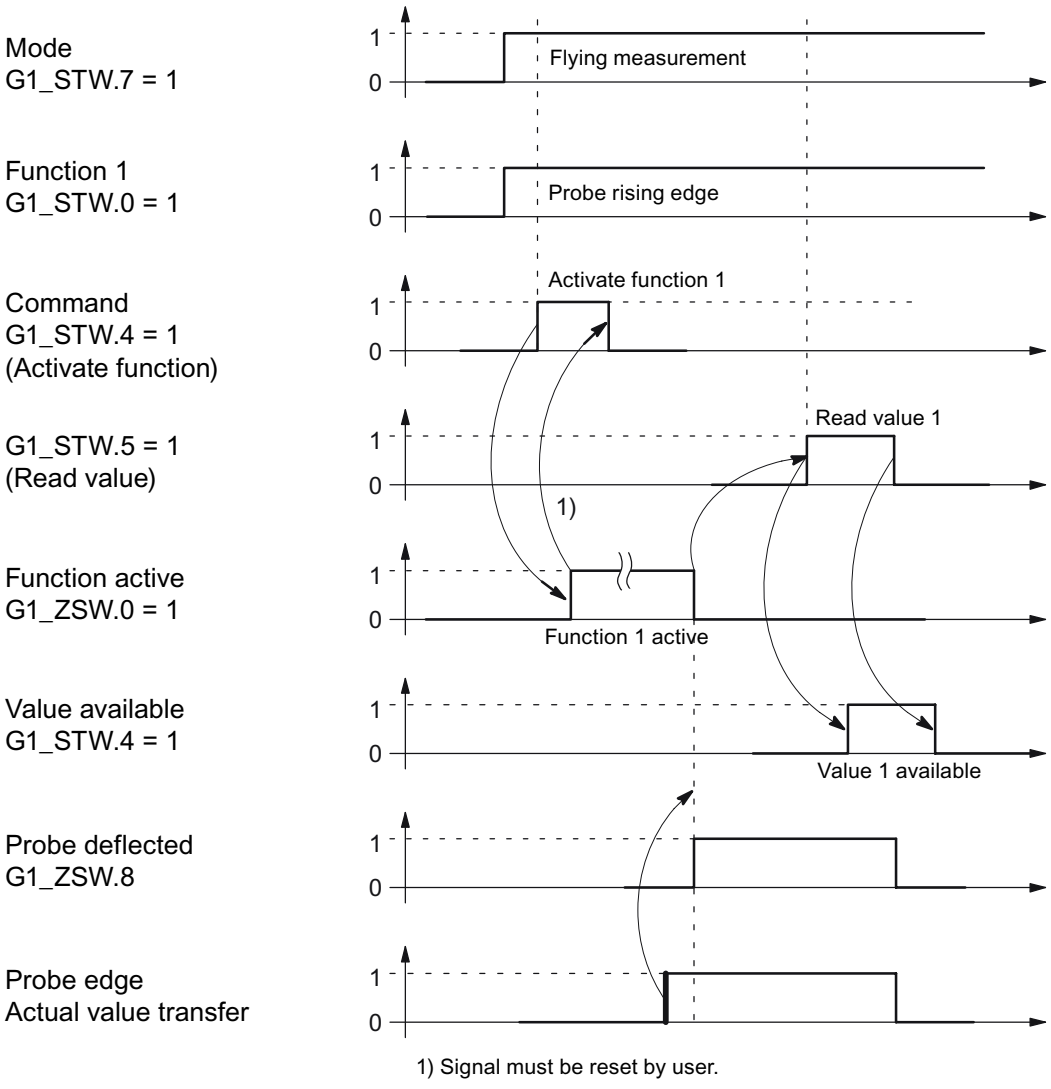


Figure A-4 Sequence chart for "Flying measurement"

Motion control with PROFIdrive

An isochronous drive coupling can be established between the control and device using the "Motion control with PROFIdrive" function.

Note

The isochronous drive coupling is defined in the following documentation:
PROFIdrive Profile Drive Technology

PROFIBUS User Organization e. V.
Haid-und-Neu-Straße 7, D-76131 Karlsruhe,
Internet: (http://www.profibus.com)

Properties

- No additional parameters need to be entered in addition to the bus configuration in order to activate this function, the master and slave must only be preset for this function (PROFIBUS).
- The controller-side default setting is made via the hardware configuration, e.g. HW Config with SIMATIC S7. The device-side default setting is made using the parameterization telegram when the bus ramps up.
- Fixed sampling times are used for all data communication.
- The Global Control (GC) clock information on PROFIBUS is sent before the beginning of each cycle.
- The cycle length depends on the bus configuration. When the cycle is selected, the bus configuration tool (e.g. HW Config) supports:
  - Large number of drives per device/drive unit → longer cycle
  - Large number of devices/ drive units → longer cycle
- A sign-of-life counter is used to monitor user data transfer and clock pulse failures.

More information

- Overview of closed-loop control (Page 81)
- Structure of the data cycle (Page 82)
- Structure of the data cycle (Page 82)

Overview of closed-loop control

- Position actual value sensing in the device is alternatively realized using an:
  - Indirect measuring system (motor encoder)
  - Additional direct measuring system
- The encoder interface must be configured in the process data.
- The control loop is closed via PROFIBUS.
- The position controller is located in the controller.
- The current and speed control and actual value sensing (encoder interface) are located in the device.
- The position controller cycle is transferred via the fieldbus to the devices.
- The slaves synchronize their speed and/or current controller sampling time with the position controller clock cycle of the controller.
- The speed setpoint is specified by the controller.

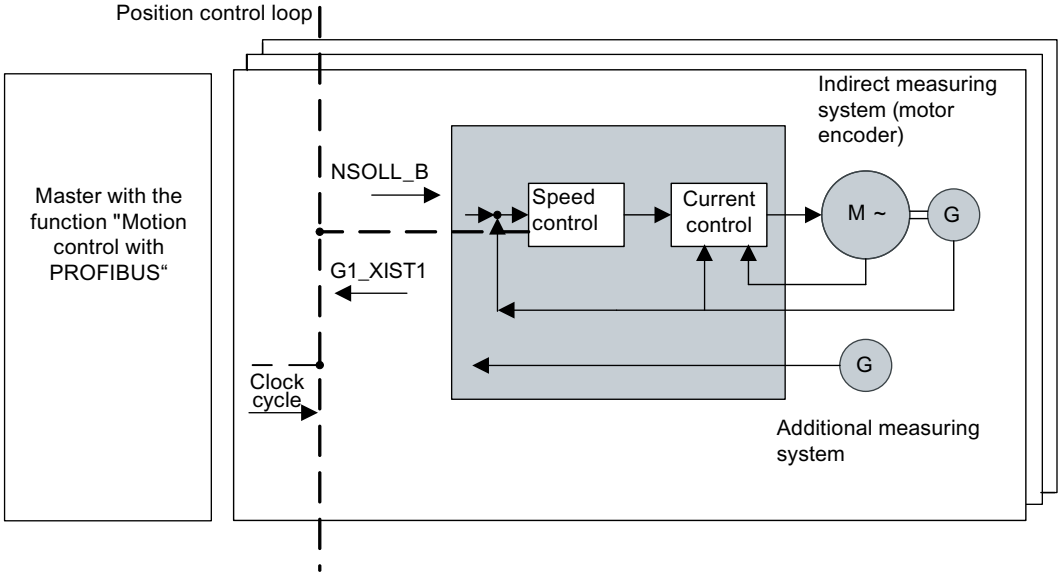


Figure A-5 Overview of "Motion Control with PROFIBUS" (example: controller and 3 devices)

Structure of the data cycle

The data cycle comprises the following elements:

- Global control telegram (PROFIBUS only)
- Cyclic part - setpoints and actual values
- Acyclic part - parameters and diagnostic data
- Reserve (PROFIBUS only)
  - Token passing (Token Holding Time, TTH)
  - For searching for a new node in the drive line-up (GAP)
  - Waiting time until start of the next cycle

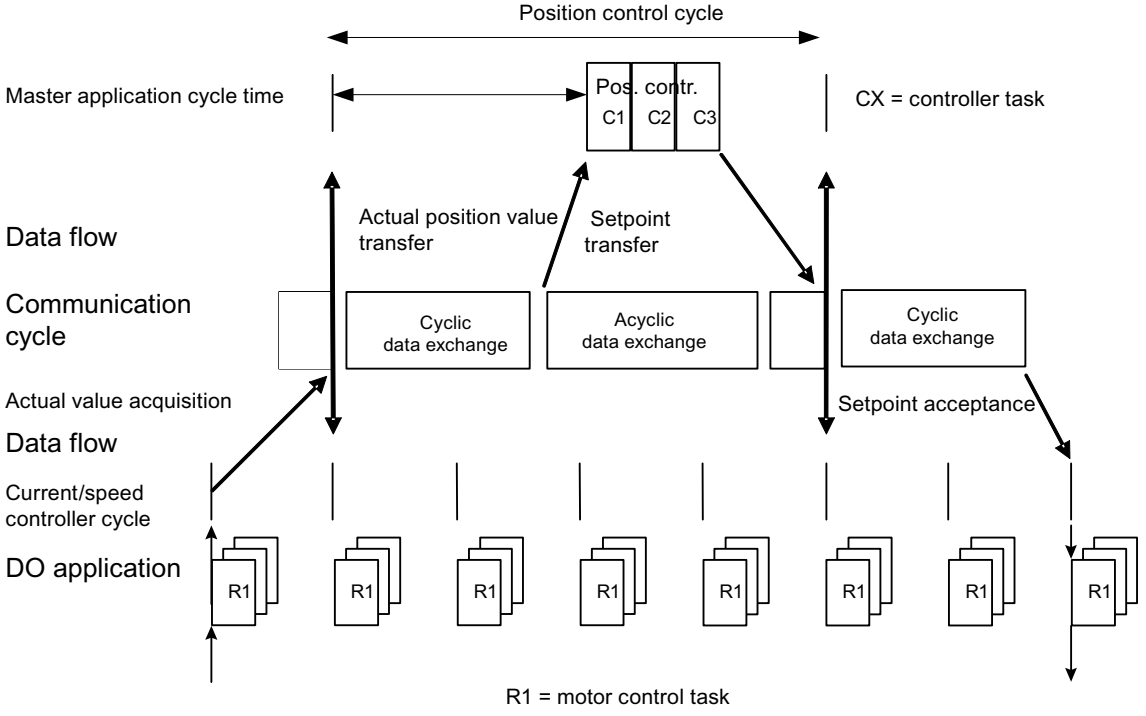


Figure A-6 Isochronous drive coupling / motion control with PROFIdrive

Overview of important parameters (see SINAMICS S120/S150 List Manual)

- p0922 IF1 PROFIdrive PZD telegram selection
- p0978[0...n] List of drive objects
- p8815[0...1] IF1/IF2 PZD functionality selection
- p8839[0...1] PZD interface hardware assignment

A.1.1.4 Parallel operation of communication interfaces

The two cyclic interfaces for the setpoints and actual values differ by the parameter ranges used (BICO technology etc.) and the functions that can be used. The interfaces are designated as cyclic interface 1 (IF1) and cyclic interface 2 (IF2).

Cyclic process data (setpoints / actual values) are processed using interfaces IF1 and IF2. The following interfaces are used:

- Onboard interfaces of the Control Unit for PROFIBUS DP or PROFINET.
- An optional interface (COMM BOARD) for PROFINET (CBE20) or CANopen (CBC10) for insertion in the Control Unit.

Parameter p8839 is used to set the parallel use of the Control Unit onboard interfaces and COMM - BOARD in the SINAMICS system. The functionality is assigned to interfaces IF1 and IF2 using indices.

For example, the following applications are possible:

- PROFIBUS DP for control and PROFINET to acquire actual values / measured values of the drive
- PROFIBUS DP for control and PROFINET for engineering only
- Mixed mode with two masters (the first for logic and coordination and the second for technology)
- SINAMICS Link via IF2 (CBE20); standard telegrams and PROFIsafe via IF1
- Operation of redundant communication interfaces

Assignment of communication interfaces to cyclic interfaces

With the factory setting p8839 = 99, the communication interfaces are permanently assigned one of the cyclic interfaces (IF1, IF2), depending on the communication system, e.g. PROFIBUS DP, PROFINET or CANopen.

The assignment to the cyclic interfaces can essentially be freely defined by user parameterization for the parallel operation of the communication interfaces.

More information

- Properties of the cyclic interfaces IF1 and IF2 (Page 84)
- Assigning the hardware for cyclic communication (Page 85)

Properties of the cyclic interfaces IF1 and IF2

Table A-5 Properties of the cyclic interfaces IF1 and IF2

Feature	IF1	IF2
Setpoint (BICO signal source)	r2050, r2060	r8850, r8860
Actual value (BICO signal sink)	p2051, p2061	p8851, p8861

Table A-6 Implicit assignment of hardware to the cyclic interfaces for p8839[0] = p8839[1] = 99

Plugged hardware interface	IF1	IF2
No option, only use Control Unit onboard interface (PROFIBUS, PROFINET or USS)	Control Unit onboard	--
CU320-2 DP with CBE20 (optional PROFINET interface)	COMM BOARD	Control Unit onboard PROFIBUS or Control Unit onboard USS
CU320-2 PN with CBE20 (optional PROFINET interface)	Control Unit onboard PROFINET	COMM BOARD PROFINET
CAN option CBC10	Control Unit onboard	COMM BOARD CAN

Parameter p8839[0,1] is used to set the parallel operation of the hardware interfaces and the assignment to the cyclic interfaces IF1 and IF2 for the Control Unit drive object.

The sequence of objects is in line with p0978 (list of drive objects) for both interfaces.

The factory setting of p8839[0,1] = 99 enables the implicit assignment (see table above).

An alarm is generated in case of invalid or inconsistent parameterization of the assignment.

Parallel operation of PROFIBUS and PROFINET

Either the isochronous mode or the PROFIsafe functionality can be assigned to an interface via p8815 (IF1 or IF2).

Example:

- p8815[0] = 1: IF1 supports the isochronous mode
- p8815[1] = 2: IF2 supports PROFIsafe

Additional parameter assignment options are possible if additionally the PROFINET module CBE20 is inserted in the CU320-2 DP:

- p8839[0] = 1 and p8839[1] = 2: PROFIBUS isochronous, PROFINET cyclic
- p8839[0] = 2 and p8839[1] = 1: PROFINET isochronous, PROFIBUS cyclic

Parameters for IF2

The following parameters are available in order to tune the IF2 for a PROFIBUS or PROFINET interface:

- Receive and send process data:
  r8850, p8851, r8853, r8860, p8861, r8863[1)]
- Diagnostic parameters:
  r8874, r8875, r8876[1)]
- Binector-connector converters:
  p8880, p8881, p8882, p8883, p8884, r8889[1)]
- Connector-binector converters:
  r8894, r8895, p8898, p8899[1)]

[1)] Meaning of 88xx is identical to 20xx (for IF1)

Note

Using the HW Config configuration tool, a PROFIBUS slave / PROFINET device with two interfaces cannot be shown. In parallel operation, this is the reason that SINAMICS drive appears twice in the project or in two projects, although physically it is just one device.

Assigning the hardware for cyclic communication

Use parameter p8839 to allocate the hardware for the cyclic communication:

p8839	PZD interface hardware assignment
Description:	Assigning the hardware for cyclic communication via PZD interface 1 and interface 2.
Values:	0: Inactive
	1: Control Unit onboard
	2: COMM BOARD
	99: Automatic

For p8839, the following rules apply:

- The setting of p8839 applies for all drive objects of a Control Unit (device parameter).
- For the setting p8839[0] = 99 and p8839[1] = 99 (automatic assignment, factory setting), the hardware used is automatically assigned to interfaces IF1 and IF2. Both indices must be selected so that the automatic assignment is activated. If both indices are not selected, then an alarm is output and the setting p8839[x] = 99 is treated just like 'inactive'.
- An alarm is issued if the same hardware (Control Unit onboard or COMM BOARD) is selected in p8839[0] and p8839[1]. The following then applies: The setting of p8839[0] is valid, and the setting of p8839[1] is treated like 'inactive'.
- If the CAN board (CBC10) is used, the entry of p8839[0] = 2 is not permissible (no assignment of the CAN board to IF1). An alarm is then issued.
- If p8839[x] is set to 2, and the COMM BOARD is missing or defective, then the corresponding interface is not supplied from the Control Unit onboard interface. Message A08550 is output instead.

A.1.1.5 Acyclic communication

General information about acyclic communication

With acyclic communication, as opposed to cyclic communication, data transfer takes place only when an explicit request is made (e.g. in order to read and write parameters).

The "Read data record" and "Write data record" services are available for acyclic communication.

The following options are available for reading and writing parameters:

- S7 protocol
  This protocol uses the Startdrive commissioning tool in online operation via PROFIBUS/ PROFINET.
- PROFIdrive parameter channel with the following data sets:
  - PROFIBUS: Data block 47 (0x002F)
    The DPV1 services are available for master class 1 and class 2.
  - PROFINET: Data block 47 and 0xB02F al global access, data set 0xB02E as local access

Note

A detailed description of acyclic communication is provided in the following reference:

- References: PROFIdrive profile
  You can obtain the current version from "PROFIBUS and PROFINET International (PI) (https://www.profibus.com/download/profidrive-profile-drive-technology/)".

Addressing:

- PROFIBUS DP
  The addressing is carried out via the logical address or the diagnostics address.
- PROFINET IO
  The addressing is only undertaken using a diagnostics address which is assigned to a module as of slot 1. Parameters cannot be accessed via socket 0.

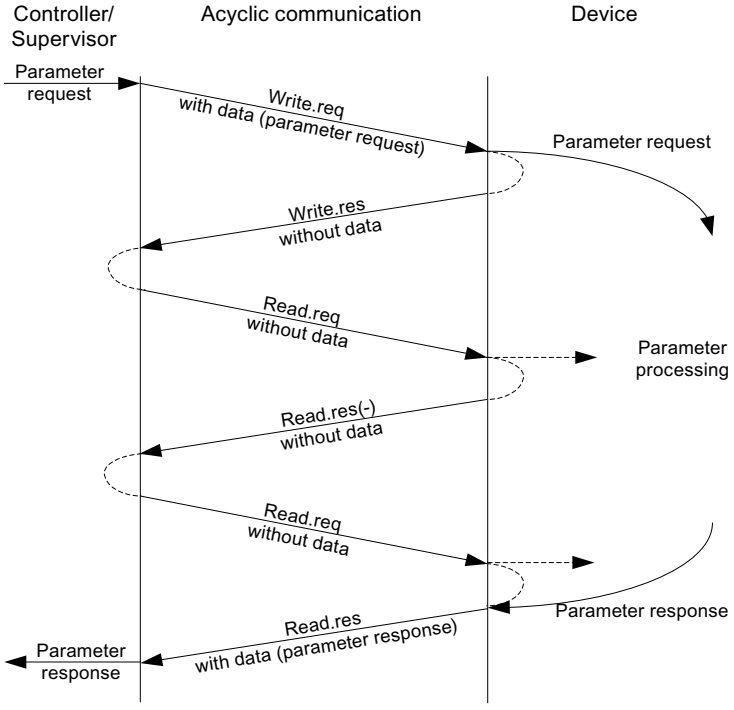


Figure A-7 Reading and writing data

Characteristics of the parameter channel

- One 16-bit address exists for each parameter number and subindex.
- Concurrent access by several additional PROFIBUS masters (master class 2) or PROFINET IO supervisor (e.g. commissioning tool).
- Transfer of different parameters in one access (multiple parameter request).
- Transfer of complete arrays or part of an array possible.
- Only one parameter request is processed at a time for each controller/device connection (no pipelining).
- A parameter request/response must fit into a data set (e.g. PROFIBUS: Max. 240 bytes).
- The request or the response header is user data.

Structure of requests and responses

Structure of parameter request and parameter response

	Parameter request			**Offset**
Values for write access only	Request header	Request reference	Request ID	0
		Axis	Number of parameters	2
	1st parameter address	Attribute	Number of elements	4
		Parameter number		6
		Subindex		8
	...			
	nth parameter address	Attribute	Number of elements	
		Parameter number		
		Subindex		
	1st parameter value(s)	Format	Number of values	
		Values		
		...		
	...			
	nth parameter value(s)	Format	Number of values	
		Values		
		...		

	Parameter response			**Offset**
Values for read access only Error values for negative response only	Response header	Request reference mirrored	Response ID	0
		Axis mirrored	Number of parameters	2
	1st parameter value(s)	Format	Number of values	4
		Values or error values		6
		...		
	...			
	nth parameter value(s)	Format	Number of values	
		Values or error values		
		...		

Description of fields in the parameter request and response

Field	**Data type**	**Values**	**Remark**
Request reference	Unsigned8	0x01 ... 0xFF	
	Unique identification of the request/response pair for the controller. The controller changes the request reference with each new request. The device mirrors the request reference in its response.		
Request ID	Unsigned8	0x01 0x02	Read request Write request
	Specifies the type of request. In the case of a write request, the changes are made in a volatile memory (RAM). A save operation is needed in order to transfer the modified data to the non-volatile memory (p0971, p0977).		
Response ID	Unsigned8	0x01 0x02 0x81 0x82	Read request (+) Write request (+) Read request (-) Write request (-)
	Mirrors the request identifier and specifies whether request execution was positive or negative. Negative means: Cannot execute part or all of request. The error values are transferred instead of the values for each subresponse.		
Drive object number	Unsigned8	0x01 ... 0xFE	Number
	Specification of the drive object number for a drive unit with more than one drive object. Different drive objects with separate parameter number ranges can be accessed over the same DPV1 connection.		
Number of parameters	Unsigned8	0x01 ... 0x27	No. 1 ... 39 Limited by DPV1 telegram length
	Defines the number of adjoining areas for the parameter address and/or parameter value for multi-parameter requests. The number of parameters = 1 for single requests.		
Attribute	Unsigned8	0x10 0x20 0x30	Value Description Text (not implemented)
	Type of parameter element accessed.		

Field	Data type	Values	Remark
Number of elements	Unsigned8	0x00 0x01 ... 0x75	Special function No. 1 ... 117 Limited by DPV1 telegram length
	Number of array elements accessed.		
Parameter number	Unsigned16	0x0001 ... 0xFFFF	No. 1 ... 65535
	Addresses the parameter to be accessed.		
Subindex	Unsigned16	0x0000 ... 0xFFFE	Number 0 ... 65534
	Addresses the first array element of the parameter to be accessed.		
Format	Unsigned8	0x02 0x03 0x04 0x05 0x06 0x07 0x08 Other values	Data type integer8 Data type integer16 Data type integer32 Data type unsigned8 Data type unsigned16 Data type unsigned32 Data type floating point See the actual PROFIdrive profile
		0x40 0x41 0x42 0x43 0x44	Zero (without values as a positive subresponse to a write request) Byte Word Double word Error
	The format and number specify the adjoining space containing values in the telegram. For write access, it is preferable to specify data types according to the PROFIdrive profile. Bytes, words and double words are also possible as a substitute.		
Number of values	Unsigned8	0x00 ... 0xEA	No. 0 ... 234 Limited by DPV1 telegram length
	Specifies the number of subsequent values.		
Error values	Unsigned16	0x0000 ... 0x00FF	Significance of the error values → refer to the following table "Error values in the DPV1 parameter responses"
	The error values in the event of a negative response. If the values make up an odd number of bytes, a zero byte is attached. This ensures the integrity of the word structure of the telegram.		
Values	Unsigned16	0x0000 ... 0x00FF	
	The values of the parameter for read or write access. If the number of bytes is odd, a zero byte is appended. This ensures the integrity of the word structure of the telegram.		

Error values in parameter responses

Error value	Meaning	Remark	Additional info
0x00	Illegal parameter number.	Access to a parameter that does not exist.	–
0x01	Parameter value cannot be changed.	Modification access to a parameter value that cannot be changed.	Subindex
0x02	Lower or upper value limit exceeded.	Modification access with value outside value limits.	Subindex

Error value	Meaning	Remark	Additional info
0x03	Invalid subindex.	Access to a subindex that does not exist.	Subindex
0x04	No array.	Access with subindex to an unindexed parameter.	–
0x05	Wrong data type.	Modification access with a value that does not match the data type of the parameter.	–
0x06	Illegal set operation (only reset allowed).	Modification access with a value not equal to 0 in a case where this is not allowed.	Subindex
0x07	Description element cannot be changed.	Modification access to a description element that cannot be changed.	Subindex
0x09	No description data available.	Access to a description that does not exist (the parameter value exists).	–
0x10	Read job will not be executed.	The read request is refused because know-how protection is active.	
0x0B	No operating priority.	Modification access with no operating priority.	–
0x0F	No text array exists.	Access to a text array that does not exist (the parameter value exists).	–
0x11	Request cannot be executed due to operating status.	Access is temporarily not possible for unspecified reasons.	–
0x14	Illegal value.	Modification access with a value that is within the limits but is illegal for other permanent reasons (parameter with defined individual values).	Subindex
0x15	Response too long.	The length of the present response exceeds the maximum transfer length.	–
0x16	Illegal parameter address.	Illegal or unsupported value for attribute, number of elements, parameter number, subindex or a combination of these.	–
0x17	Illegal format.	Write request: Illegal or unsupported parameter data format.	–
0x18	Number of values inconsistent.	Write request: A mismatch exists between the number of values in the parameter data and the number of elements in the parameter address.	–
0x19	Drive object does not exist.	You have attempted to access a drive object that does not exist.	–
0x20	Parameter text cannot be changed	–	–
0x21	Service not supported.	Illegal or unknown request ID	–
0x65	Parameter presently deactivated.	You have tried to access a parameter that, although available, does not currently perform a function (e.g. n control set and access to a V/f control parameter).	–
0x6B	Write access for enabled controller.	Write access is possible while the device is in the "Controller enable" state. Pay attention to the parameter attribute "changeable" in the SINAMICS S120/S150 List Manual (C1, C2, U, T).	–
0x6C	Parameter %s [%s]: Unknown unit.	–	–
0x6D	Parameter %s [%s]: Write access only in the commissioning state, encoder (p0010 = 4).	–	–
0x6E	Parameter %s [%s]: Write access only in the commissioning state, motor (p0010 = 3).	–	–

Error value	Meaning	Remark	Additional info
0x6F	Parameter %s [%s]: Write access only in the commissioning state, power unit (p0010 = 2).	–	–
0x70	Parameter %s [%s]: Write access only in the quick commissioning mode (p0010 = 1).	–	–
0x71	Parameter %s [%s]: Write access only in the ready mode (p0010 = 0).	–	–
0x72	Parameter %s [%s]: Write access only in the commissioning state, parameter reset (p0010 = 30).	–	–
0x73	Parameter %s [%s]: Write access only in the commissioning state, Safety (p0010 = 95).	–	–
0x74	Parameter %s [%s]: Write access only in the commissioning state, tech. application/units (p0010 = 5).	–	–
0x75	Parameter %s [%s]: Write access only in the commissioning state (p0010 not equal to 0).	–	–
0x76	Parameter %s [%s]: Write access only in the commissioning state, download (p0010 = 29).	–	–
0x77	Parameter %s [%s] must not be written during download.	–	–
0x78	Parameter %s [%s]: Write access only in the commissioning state, drive configuration (device: p0009 = 3).	–	–
0x79	Parameter %s [%s]: Write access only in the commissioning state, define drive type (device: p0009 = 2).	–	–
0x7A	Parameter %s [%s]: Write access only in the commissioning state, data record base configuration (device: p0009 = 4).	–	–
0x7B	Parameter %s [%s]: Write access only in the commissioning state, device configuration (device: p0009 = 1).	–	–
0x7C	Parameter %s [%s]: Write access only in the commissioning state, device download (device: p0009 = 29).	–	–
0x7D	Parameter %s [%s]: Write access only in the commissioning state, device parameter reset (device: p0009 = 30).	–	–
0x7E	Parameter %s [%s]: Write access only in the commissioning state, device ready (device: p0009 = 0).	–	–

Error value	Meaning	Remark	Additional info
0x7F	Parameter %s [%s]: Write access only in the commissioning state, device (device: p0009 not equal to 0).	–	–
0x81	Parameter %s [%s] must not be written during download.	–	–
0x82	Transfer of master control is blocked by BI: p0806.	–	–
0x83	Parameter %s [%s]: Requested BICO interconnection not possible.	BICO output does not supply float values. The BICO input, however, requires a float value.	–
0x84	Parameter %s [%s]: Parameter change inhibited (refer to p0300, p0400, p0922)	–	–
0x85	Parameter %s [%s]: Access method not defined.	–	–
0x87	Write job will not be executed.	The write request is rejected because know-how protection is active.	–
0xC8	Below currently valid limit.	Modification request for a value that, although within "absolute" limits, is below the currently valid lower limit.	–
0xC9	Above currently valid limit.	Modification request for a value that, although within "absolute" limits, is above the currently valid upper limit (e.g. governed by the current converter rating).	–
0xCC	Write access not permitted.	Write access is not permitted because an access code is not available.	–

Determining the drive object numbers

Further information about the drive system (e.g. drive object numbers) can be determined as follows using parameters p0101, r0102, and p0107/r0107:

1. The value of parameter r0102 ("Number of drive objects") for drive object/axis 1 is read via a read request.
   Drive object 1 is the Control Unit (CU) which is a minimum requirement for each drive system.
2. Depending on the result of the initial read request, further read requests for drive object 1 are used to read the indices for parameter p0101 "Drive object numbers", as specified by parameter r0102.
   Example:
   If the number of drive objects is "5", the values of indices 0 to 4 of parameter p0101 are read.
   Of course, the relevant indexes can also be read at once.
3. Following this, parameter r0107/p0107 ("Drive object type") is read for each drive object/axis (indicated by the drive object number).
   Depending on the drive object, parameter 107 can be either an adjustable parameter or a display parameter.
   The value in parameter r0107/p0107 indicates the drive object type. The coding for the drive object type is specified in the parameter list.

Example 1: read parameters

Requirements

- The PROFIdrive controller has been commissioned and is fully operational.
- PROFIdrive communication between the controller and the device is operational.
- The controller can read and write data sets in conformance with PROFINET/PROFIBUS.

Task description

Following the occurrence of at least one fault (ZSW1.3 = "1") on drive 2 (also drive object number 2), the active fault codes must be read from the fault buffer r0945[0] ... r0945[7].

The request is to be handled using a request and response data block.

Basic procedure

1. Create a request to read the parameters.
2. Invoke the request.
3. Evaluate the response.

Create the request

Parameter request			**Offset**
Request header	Request reference = 25 hex	Request ID = 01 hex	0 + 1
	Axis = 02 hex	Number of parameters = 01 hex	2 + 3
Parameter address	Attribute = 10 hex	Number of elements = 08 hex	4 + 5
	Parameter no. = 945 dec		6
	Subindex = 0 dec		8

Information about the parameter request:

- Request reference:
  The value is selected at random from the valid value range. The request reference establishes the relationship between request and response.
- Request ID:
  01 hex → This identifier is required for a read request.
- Axis:
  02 hex → Drive 2, fault buffer with drive- and device-specific faults.
- Number of parameters:
  01 hex → One parameter is read.
- Attribute:
  10 hex → The parameter values are read.
- Number of elements:
  08 hex → The actual fault incident with eight faults is to be read.

- Parameter number:
  945 dec → p0945 (fault code) is read.
- Subindex:
  0 dec → Reading starts at index 0.

Initiate parameter request.

If ZSW1.3 = "1" → Initiate parameter request

Evaluate the parameter response.

Parameter response			**Offset**
Response header	Request reference mirrored = 25 hex	Response ID = 01 hex	0 + 1
	Axis mirrored = 02 hex	Number of parameters = 01 hex	2 + 3
Parameter value	Format = 06 hex	Number of values = 08 hex	4 + 5
	1st value = 1355 dec		6
	2nd value = 0 dec		8
	...		...
	8th value = 0 dec		20

Information about the parameter response:

- Request reference mirrored:
  This response belongs to the request with request reference 25.
- Response ID:
  01 hex → Read request positive, values stored as of 1st value.
- Axis mirrored, number of parameters:
  The values correspond to the values from the request.
- Format:
  06 hex → Parameter values are in the unsigned16 format.
- Number of values:
  08 hex → Eight parameter values are available.
- 1st value ... 8th value
  A fault is only entered in value 1 of the fault buffer for drive 2.

Example 2: Writing parameters (multi-parameter request)

Requirements

- The PROFIdrive controller has been commissioned and is fully operational.
- PROFIdrive communication between the controller and the device is operational.

- The controller can read and write data sets in conformance with PROFINET/PROFIBUS.
- Special requirements for this example:
  Servo control or vector control with activated "Extended setpoint channel" function module

Task description

Jog 1 and 2 are to be set up for drive 2 (also drive object number 2) via the input terminals of the Control Unit. A parameter request is to be used to write the corresponding parameters as follows:

- BI: p1055 = r0722.4 — Jog bit 0
- BI: p1056 = r0722.5 — Jog bit 1
- p1058 = 300 rpm — Jog 1 speed setpoint
- p1059 = 600 rpm — Jog 2 speed setpoint

The request is to be handled using a request and response data block.

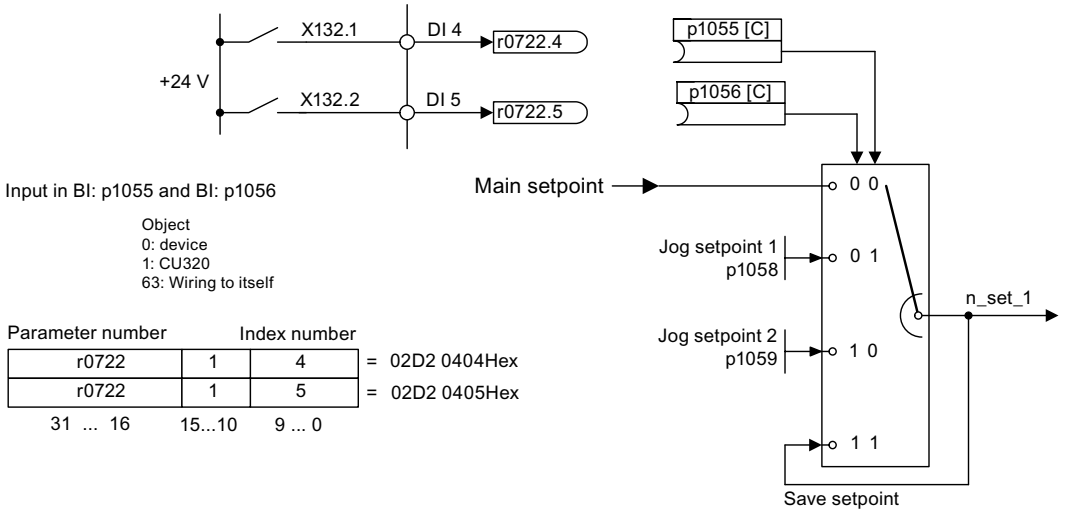


Figure A-8 Task description for multi-parameter request (example)

Basic procedure

1. Create a request to write the parameters.
2. Invoke the request.
3. Evaluate the response.

Create the request

Parameter request			**Offset**
Request header	Request reference = 40 hex	Request ID = 02 hex	0 + 1
	Axis = 02 hex	Number of parameters = 04 hex	2 + 3

Parameter request			Offset
1st parameter address	Attribute = 10 hex	Number of elements = 01 hex	4 + 5
	Parameter no. = 1055 dec		6
	Subindex = 0 dec		8
2nd parameter address	Attribute = 10 hex	Number of elements = 01 hex	10 + 11
	Parameter no. = 1056 dec		12
	Subindex = 0 dec		14
3rd parameter address	Attribute = 10 hex	Number of elements = 01 hex	16 + 17
	Parameter no. = 1058 dec		18
	Subindex = 0 dec		20
4th parameter address	Attribute = 10 hex	Number of elements = 01 hex	22 + 23
	Parameter no. = 1059 dec		24
	Subindex = 0 dec		26
1st parameter value(s)	Format = 07 hex	Number of values = 01 hex	28 + 29
	Value = 02D2 hex		30
	Value = 0404 hex		32
2nd parameter value(s)	Format = 07 hex	Number of values = 01 hex	34 + 35
	Value = 02D2 hex		36
	Value = 0405 hex		38
3rd parameter value(s)	Format = 08 hex	Number of values = 01 hex	40 + 41
	Value = 4396 hex		42
	Value = 0000 hex		44
4th parameter value(s)	Format = 08 hex	Number of values = 01 hex	46 + 47
	Value = 4416 hex		48
	Value = 0000 hex		50

Information about the parameter request:

- Request reference:
  The value is selected at random from the valid value range. The request reference establishes the relationship between request and response.
- Request ID:
  02 hex → This identifier is required for a write request.
- Axis:
  02 hex → The parameters are written to drive 2.
- Number of parameters
  04 hex → The multi-parameter request comprises four individual parameter requests.

1st parameter address ... 4. Parameter address

- Attribute:
  10 hex → The parameter values are to be written.
- Number of elements
  01 hex → One array element is written.

- Parameter number
  Specifies the number of the parameter to be written (p1055, p1056, p1058, p1059).
- Subindex:
  0 dec → ID of the first array element.

1st parameter value ... 4th Parameter value

- Format:
  07 hex → Data type, unsigned32
  08 hex → Data type, floating point
- Number of values:
  01 hex → A value is written to each parameter in the specified format.
- Value:
  BICO input parameter: Enter signal source
  Adjustable parameter: Enter value

Initiate parameter request.

If ZSW1.3 = "1" → Initiate parameter request

Evaluate the parameter response.

Parameter response			**Offset**
Response header	Request reference mirrored = 40 hex	Response ID = 02 hex	0
	Axis mirrored = 02 hex	Number of parameters = 04 hex	2

Information about the parameter response:

- Request reference mirrored:
  This response belongs to the request with request reference 40.
- Response ID:
  02 hex → Write request positive
- Axis mirrored:
  02 hex → The value matches the value from the request.
- Number of parameters:
  04 hex → The value matches the value from the request.

A.1.1.6 Diagnostics channels

SINAMICS drives provide the standard diagnostics for PROFIBUS and PROFINET. This allows the PROFIdrive classes of the SINAMICS drive to be integrated into the system diagnostics of a higher-level control system and automatically displayed on an HMI.

The information transferred is saved for the drive objects in the following parameters:

- r0947[0...63] fault number
- r2122[0...63] alarm code
- r9747[0...63] SI message code (with safety messages)
- r3120[0..63] component fault
- r3121[0..63] component alarm
- r9745[0..63] SI component (with safety message)

The messages entered in these parameters are combined to create PROFIdrive message classes for diagnostics. Determining the source of a message is realized by transferring the component number as channel number.

The diagnostics are activated through appropriate parameterization in the configuring tools used (e.g. using HW Config or via HWCN in the TIA Portal).

The functional scope of the diagnostic channels depends on the bus system.

		PROFIdrive message classes		
		Faults	**Alarms**	**Component assignment**
PN	GSDML	X	X	X
	TIA	X	X	X
DP	GSD	X	-	-
	TIA	X	-	-

- SINAMICS transfers the messages in the sequence in which they occurred.
- If an alarm appears, SINAMICS sends an "incoming" message. The alarm remains until SINAMICS sends the corresponding "outgoing" message.
- The time stamps are generated from the higher-level controller when the messages are received
- The existing mechanisms of TIA and S7 Classic can be used.
- Alarms or faults are acknowledged using the already known acknowledgment routes.
- Transfer is possible via interface IF1 and/or IF2.

Note

Constraint

If a shared device is activated, only the A-controller can receive diagnostics.

Note

Additional information

PROFIdrive message classes of the individual SINAMICS faults and alarms are provided in the SINAMICS List Manuals.

PROFINET-based diagnostics

For PROFINET, to transfer PROFIdrive message classes, channel diagnostics (Channel Diagnosis) are used (see PROFINET IO specification (http://www.profibus.com)).

A message always comprises the following components in this specific sequence:

- Block Header (6 Byte)
  - Blocktype
  - Blocklength
  - BlockversionHigh
  - BlockversionLow
- API (4 Byte)
- Slot Number (2 Byte)
- Sub Slot Number (2 Byte)
- Channel Number (2 Byte)
- Channel Properties (0x8000) (2 Byte)
- User Structure Identifier (2 Byte)
- Channel Diagnosis Data (6 Byte)
  - Channel Number (2 Byte)
  - Channel Properties (2 Byte)
  - Channel Error Type (2 Byte)

More information

- Message components (Page 100)
- System response - reading out diagnostics data (Page 102)

Message components

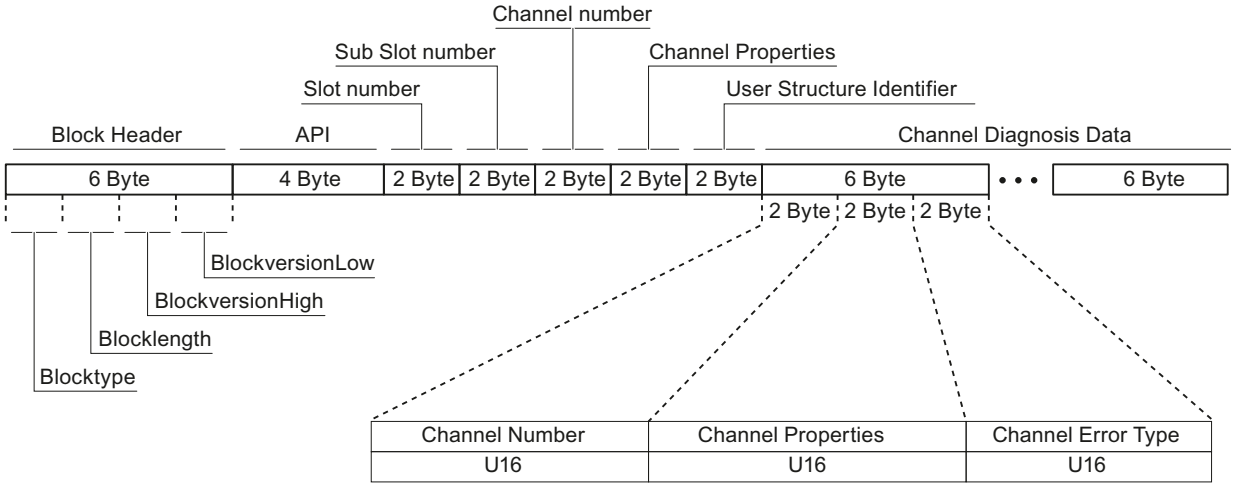


Figure A-9 Components of a message

Explanation of these message components

Individual components of the Channel Diagnosis Data block can be included n times in a message. A precise explanation of these message components is subsequently provided:

Designation		Data type/ length	For SINAMICS	
			Value	Significance
Channel Number		U16	1 ... 399	Component number
			0x8000	No component assignment[1)]
Channel Properties		U16		
	.Type	Bits 7 ... 0	0	No data length
	.Accumulative	Bit 8	0	1 channel; no group formation
	.Maintenance	Bits 10, 9	0	Fault → diagnostics
			1	Alarm, Class 0 or A → maintenance *required* Alarm, Class B or C → maintenance *demanded*
			2	
	.Specifier	Bits 12, 11	0	Not used
			1	Message received
			2	Message issued, no additional message available in the channel
			3	Message issued, additional messages are available in the channel
	.Direction	Bits 15 ... 13	3	Input/Output
Channel Error Type		U16	0x9000	Hardware / software error
			0x9001	Network fault
			0x9002	Supply voltage fault
			0x9003	DC link overvoltage
			0x9004	Power electronics faulted
			0x9005	Overtemperature of the electronic components
			0x9006	Ground fault / inter-phase short circuit
			0x9007	Motor overload
			0x9008	Communication error to the higher-level control system
			0x9009	Safety monitoring channel has identified an error
			0x900A	Position/speed actual value incorrect or not available
			0x900B	Internal (DRIVE-CLiQ) communication error
			0x900C	Infeed faulted
			0x900E	Line filter faulted
			0x900F	External measured value / signal state outside the permissible range
			0x9010	Application / technological function faulted
			0x9011	Error in the parameterization / configuration / commissioning procedure
			0x9012	General drive fault
			0x9013	Auxiliary unit faulted

[1)] For messages, which cannot be assigned to any particular component

System response - reading out diagnostics data

The converter can request diagnostics data via "Read data set" (detailed information is provided in the PROFINET-IO specification (http://www.profibus.com)).

Example:

For example, a read record with index 0x800C can be used to read out diagnostics data from specific sub slots. The following rules apply as example:

- 1 message block
  if, at this drive object (one or several) faults of the same message class are identified
- n messages
  if, at this drive object, n faults of different message classes are identified

Note

If a fault is active on the CU drive object, then this fault is propagated to all of the drive objects associated with the CU. This fault can therefore be read out at each drive object.

PROFIBUS-based diagnostics

For communication via PROFIBUS, in the case of fault the following diagnostics data is output:

- Standard diagnostics (Page 103)
- Identifier-related diagnostics (Page 104)
- Status messages/module status (Page 104)
- Channel-related diagnostics (Page 105)
- Data sets DS0/DS1 and diagnostics alarm (Page 106)

Message structure

The following applies if a message contains all of the specified diagnostics data:

- Standard diagnostics
  Is always located at the beginning of the message.
- Data sets DS0/DS1 and diagnostics alarm
  Is always located at the end of the message. This message part is always slot-specific. The actual state of the slot responsible for the message is always transferred in the message.

The other diagnostics data (types) can be in any sequence. This is the reason that the following diagnostics data include a header:

- Identifier-related diagnostics
- Status messages/module status
- Channel-related diagnostics

The diagnostic data type can be uniquely identified based on the header.

Note

The master must operate in the DPV1 mode.

Standard diagnostics

For communication via PROFIBUS, standard diagnostics is structured as follows.

	Bit	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
Octet	**Name**								
1	Station status 1	Master_ Lock = 0	Prm_Fault	0	Not_ Supported	**Ext_Diag**	Cfg_Fault	Station_ Not_ Ready	Station_ Non_ Exist = 0
2	Station status 2	0	0	Sync_ Mode	Freeze_ Mode	WD_On	1	**Stat_Diag** = 0	Prm_Req
3	Station status 3	**Ext_ Diag_ Overflow**	0	0	0	0	0	0	0
4		Master_Add							
5		Ident_Number (HighByte) of the slave							
6		Ident_Number (LowByte) of the slave							

In this context, the following values are decisive for diagnostics:

- Ext_Diag
  - Group signal for diagnostics in the slave
  - = 1, if at least 1 alarm is active
- Ext_Diag_Overflow
  Display, diagnostics overflow in the slave (for more than 240 bytes)

Identifier-related diagnostics

The identifier-related diagnostics provides a bit (KB_n) for each slot 1 allocated when configuring the device. If a diagnostics message is active at a slot, then it's KB_n = true.

Bit		7	6	5	4	3	2	1	0
Octet	**Name**								
1	Header-Byte Station status 1	0	1	Block length (2 ... 32) incl. this byte					
2	Bit structure	KB_7	KB_6	KB_5	KB_4	KB_3	KB_2	KB_1	KB_0
3	Bit structure	...	...	...	...	KB_11	KB_10	KB_9	KB_8
...		...							
x	Bit structure	...	...	KB_n+1	KB_n	...	...	...	...

Status messages/module status

Status messages and module status briefly represent an overview of the state of the devices:

Bit		7	6	5	4	3	2	1	0
Octet	**Name**								
1	Header byte	0	0	Block length (2 ... 32) incl. this byte					
2	Module status	0x82							
3	Slot	0							
4	Specifier	0							
5		Slot_4		Slot_3		Slot_2		Slot_1	
6		...		Slot_7		Slot_6		Slot_5	
...		...							
x		00		Slot_n		...		...	

Note

Status value

Diagnostics for SINAMICS are only available in cyclic PROFIBUS operation, so that the state 00 = "Valid useful data" is always output for all slots.

Channel-related diagnostics

Channel-related diagnostics encompasses the following data:

Bit		7	6	5	4	3	2	1	0
Octet	**Name**								
x	Header-Byte	1[1]	0[1]	0 ... 63 (module number) including this byte					
x + 1		1[2]	1[2]	0 (no component assignment)					
x + 2		0[3]	0[3]	Message classes: 2 undervoltage 3 overvoltage 9 error 16 Hardware/software error 17 Line supply/filter faulted 18 DC-link overvoltage 19 Power electronics faulted 20 Electronic component overtemp. 21 Ground/phase fault detected 22 Motor overload 23 Commun. with controller faulted 24 Safety monit. Detected an error 25 Act. Position/speed value error 26 Internal communication faulted 27 Infeed faulted 28 Braking controller faulted 29 External signal state error 30 Application/function faulted 31 Parameterization/commiss. error					

1) ≙ Channel-related diagnostics

2) ≙ Input/output

3) ≙ "Channel type "non specific"

System response

Only one signal is generated if channel-related diagnostics identifies several faults belonging to the same message class at the same drive object.

Data sets DS0/DS1 and diagnostics alarm

The PROFIdrive message classes are transferred using diagnostic alarm DS0/DS1. All faults are assigned channel 0. The drive objects are assigned using the slot number.

The structure is as follows:

Bit		7	6	5	4	3	2	1	0
Octet	**Name**								
1	Header-Byte	0	0	= 15 (block length)					
2		0	= 1 (diagnostics alarm)						
3		0 ... 244 (slot number ≙ drive object)							
4		0 ... 31 (sequence number)					Add_Ack	Alarm_Specifier[1]	
5	DS0 (byte 0)	0	0	0	0	1[2]	0	1[3]	1[4]
6	DS0 (byte 1)	0	0	0	1[5]	0[6]	0[6]	1[6]	1[6]
7	DS0 (Byte 2)	0	0	0	0	0	0	0	0
8	DS0 (byte 3)	0	0	0	0	0	0	0	0
9	Info (byte 1)	Mixed	= 0x45 (ChannelTypeID = SINAMICS)						
10	Info (byte 2)	= 24 (number of diagnostic bits/channel)							
11	Info (byte 3)	= 1 (1 channel signals)							
12	Channel Error Vector	0	0	0	0	0	0	0	Channel 0 1
13	Channel -related diag-nostics (channel 0)	Err 7	Err 6	Err 5	Err 4	Err 3	Err 2	Err 1	Err 0
14		Err 15	Err 14	Err 13	Err 12	Err 11	Err 10	Err 9	Err 8
15		0	0	0	0	Err 19	Err 18	Err 17	Err 16

1) Alarm_Specifier
1 ≙ error has occurred and the slot is not OK
2 ≙ error is resolved and the slot is OK
3 ≙ error is resolved and the slot is not okay

2) Channel fault present
= 1; as long as the drive object has an error condition

3) Internal fault
= 1; as long as the drive object has an error condition

4) Module fault
= 1; as long as the drive object has an error condition

5) Channel information present
= 1; ≙ DS1 exists

6) Type class of module
= 0011; ≙ Distributed

A.1.1.7 Configuring telegrams in Startdrive

If communication is established between the drive and higher-level control system via PROFINET IO, then the data (setpoints and actual values) are cyclically transferred using PROFIdrive telegrams.

To configure a cyclic data transfer, proceed as follows:

- Insert the drive and controller
- Insert a PROFINET subnet
- Assign the drive to the controller
- Check the bus settings
- Parameterize the drive
  You must create telegrams for the relevant drive objects, e.g. for drive axes, drive control or infeed
- Check and edit the telegram settings
- If you are controlling a drive with safety functions via PROFIsafe, you must insert the appropriate PROFIsafe telegram.

Displaying telegram configuration

The "Telegram configuration" screen form is part of the device configuration and is displayed in the inspector window.

You can call this screen form, either via the project navigation or via direct links from the communication screen forms.

Call the telegram configuration via the project navigation

1. Open the drive device in the project navigation.
2. Double-click on the entry "Device configuration."
   The device configuration opens.
3. Select the entry "Telegram configuration" in the "Properties" tab of the inspector window.
   The telegram configuration settings are displayed under the respective fieldbus interface

Dialog overview

The dialog box for the telegram configuration is structured as follows:

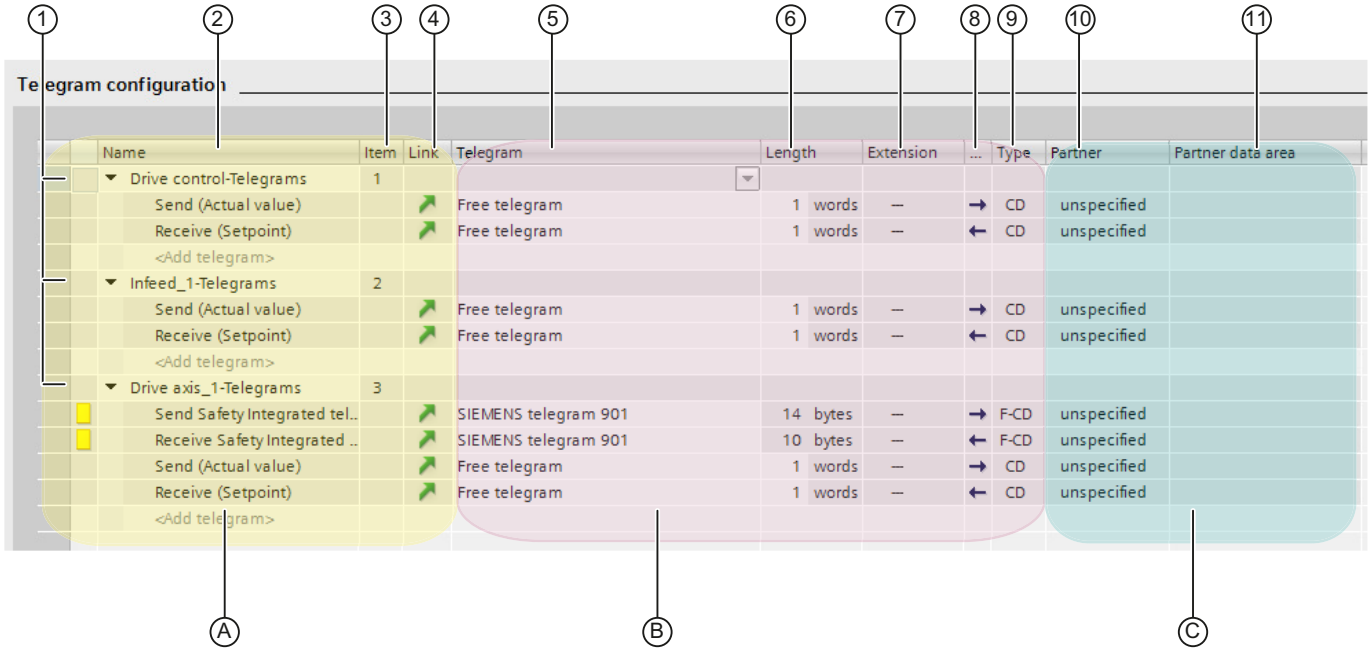


Figure A-10 Example: Telegram configuration with several drive objects

Number	Description	
A	Area for the drive objects (setpoints, actual values and safety components). A telegram is assigned to each drive object for setpoints and actual values. "Free telegram" is selected by default.	
B	Area for the interfaces	
C	Area for the communication partners of the drive (e.g. controller or another drive)	
①	Header of a drive object Using the header, you can move the drive object in the list with drag and drop (in the first column). This changes the sorting in the table and at the same time in the secondary navigation of the telegram configuration.	
②	Display of the drive object	
③	Number of the drive object This number is generated automatically according to the order in which a drive object is created in the device configuration, and can no longer be changed. Resorting in the table does not change this number.	
④	Link to the communication screen forms of the particular drive object	
⑤	Drop-down list with the available telegrams	
⑥	Telegram length	
⑦	Telegram extension	
⑧	Communication direction (send direction →/receive direction ←)	
⑨	Type of communication	CD = Controller - Device for PROFINET IO
		F_ = PROFIsafe-specific extension (safety telegram)
⑩	Name of the partner (controller)	
⑪	I/O addresses of the controller	

A.1.2 Communication via PROFIBUS DP

A.1.2.1 General information about PROFIBUS

General information about PROFIBUS for SINAMICS

PROFIBUS is an open international fieldbus standard for a wide range of production and process automation applications.

The following standards ensure open, multi-vendor systems:

- International standard EN 50170
- International standard IEC 61158

PROFIBUS is tuned for high-speed, time-critical data communication at field level.

Note

PROFIBUS for drive technology is standardized and described in the following document:
PROFIdrive Profile Drive Technology

PROFIBUS User Organization e. V.
Haid-und-Neu-Strasse 7, D-76131 Karlsruhe

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

Note

Startdrive

Please note that you still cannot use this function with Startdrive.

Note

Before synchronizing to the isochronous PROFIBUS, all of the drive object pulses must be inhibited - also for those drives that are not controlled via PROFIBUS.

PROFIBUS interface: The cyclic PZD channel is deactivated when the **CBE20** is plugged in!

NOTICE
Destruction of the CU320-2 or other CAN bus nodes by connecting a CAN cable Connecting a CAN cable to interface X126 of the CU320-2 can destroy the CU320-2 or other CAN bus nodes. • Do not connect any CAN cable to the X126 interface.

Master and slave

- Master and slave properties

Properties	Master	Slave
As bus node	Active	Passive
Send messages	Permitted without external request	Only possible on request by master
Receive messages	Possible without any restrictions	Only receive and acknowledge permitted

- Master
  The following classes are differentiated:
  - Master class 1 (DPMC1):
    Central automation stations that exchange data with the slaves in cyclic and acyclic mode. Communication between the masters is also possible.
    Examples: SIMATIC S7, SIMOTION
  - Master class 2 (DPMC2):
    Devices for configuration, commissioning, operator control and monitoring during bus operation. Devices that only exchange data with the slaves in acyclic mode.
    Examples: Programming devices, human machine interfaces
- Slaves
  With respect to PROFIBUS, the SINAMICS drive unit is a slave.

Bus access method

PROFIBUS uses the token passing method, i.e. the active stations (masters) are arranged in a logical ring in which the authorization to send is received within a defined time frame.

Within this time frame, the master with authorization to send can communicate with the assigned slaves and/or with other masters in a master/slave procedure.

PROFIBUS telegram for cyclic data transmission and acyclic services

Each drive unit that supports cyclic process data exchange uses a telegram to send and receive all the process data. A separate telegram is sent in order to perform all the acyclic services (read/write parameters) under a single PROFIBUS address. The acyclic data is transferred with a lower priority after cyclic data transmission.

The overall length of the telegram increases with the number of drive objects that are involved in exchanging process data.

Sequence of drive objects in the telegram

On the drive side, the sequence of drive objects in the telegram is displayed via a list in p0978[0...24] where it can also be changed.

Using the Startdrive commissioning tool you can display the sequence of drive objects for a commissioned drive system in the project navigator under "Drive unit" **>** "Communication" > "Telegram configuration".

When you create the configuration on the controller side (e.g. HW Config), the process-data-capable drive objects for the application are added to the telegram in the sequence shown (see above).

The following drive objects can exchange process data:

- Active Infeed (A_INF)
- Basic Infeed (B_INF)
- Control Unit (CU_S)
- ENC
- Smart Infeed (S_INF)
- SERVO
- VECTOR
- Terminal Board 30 (TB30)
- Terminal Module 15 (TM15)
- Terminal Module 31 (TM31)
- Terminal Module 41 (TM41)
- Terminal Module 120 (TM120)
- Terminal Module 150 (TM150)

Note

The sequence of drive objects in HW Config must be the same as that in the drive (p0978).

Drive objects after the first zero in p0978 must not be configured in the HW Config.

The structure of the telegram depends on the drive objects taken into account during configuration. Configurations are permitted that do not take into account all of the drive objects that are present in the drive system.

Example:

The following configurations are possible:

- Configuration with SERVO, SERVO, SERVO
- Configuration with A_INF, SERVO, SERVO, SERVO, TB30
- ...

Example: telegram structure for cyclic data transmission

Task

The drive system comprises the following drive objects:

- Control Unit (CU_S)
- Active Infeed (A_INF)
- SERVO 1 (comprises a Single Motor Module and other components)
- SERVO 2 (comprises a Double Motor Module terminal X1 and other components)
- SERVO 3 (comprises a Double Motor Module terminal X2 and other components)
- Terminal Board 30 (TB30)

The process data is to be exchanged between the drive objects and the higher-level automation system.

Telegrams to be used:

- Telegram 370 for Active Infeed
- Standard telegram 6 for SERVO
- User-defined for Terminal Board 30 for the three SERVO drives

Component and telegram structure

The predefined component structure results in the telegram structure shown in the following diagram.

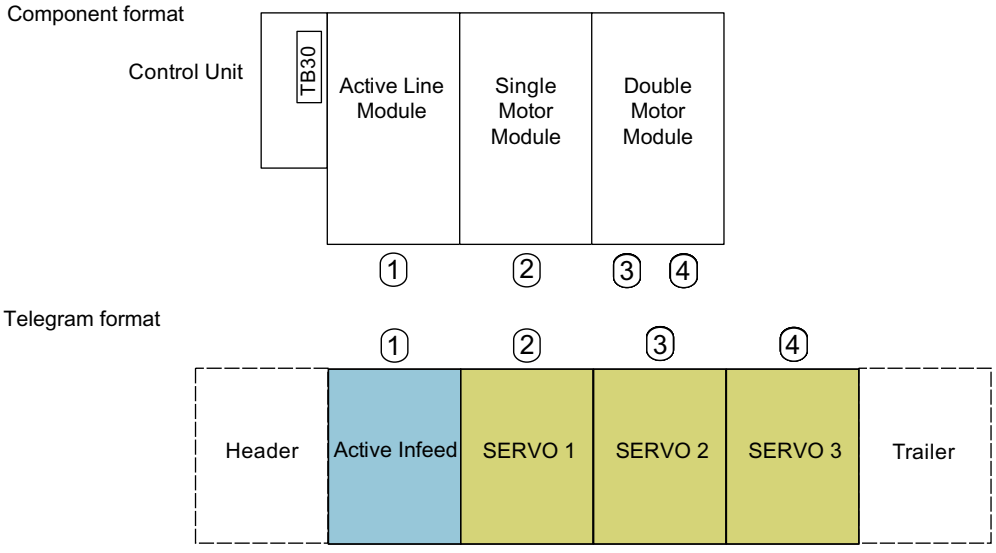


Figure A-11 Component and telegram structure

You can check and change the sequence of the telegrams via p0978[0...24].

Configuration settings (e.g. HW Config for SIMATIC S7)

Due to the telegram structure shown, the objects in the "DP slave properties" overview must be configured as follows:

- Active Infeed (A_INF): Telegram 370
- SERVO 1: Standard telegram 6
- SERVO 2: Standard telegram 6
- SERVO 3: Standard telegram 6
- Terminal Board 30 (TB30): User-defined

DP slave properties – overview

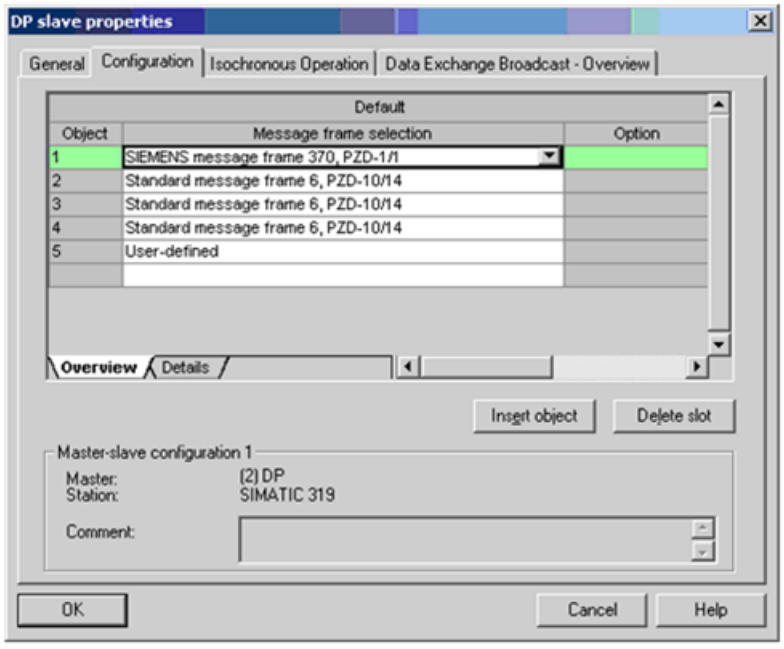


Figure A-12 Slave properties – overview

When you click "Details", the properties of the configured telegram structure are displayed (e.g. I/O addresses, axis separator).

DP slave properties – details

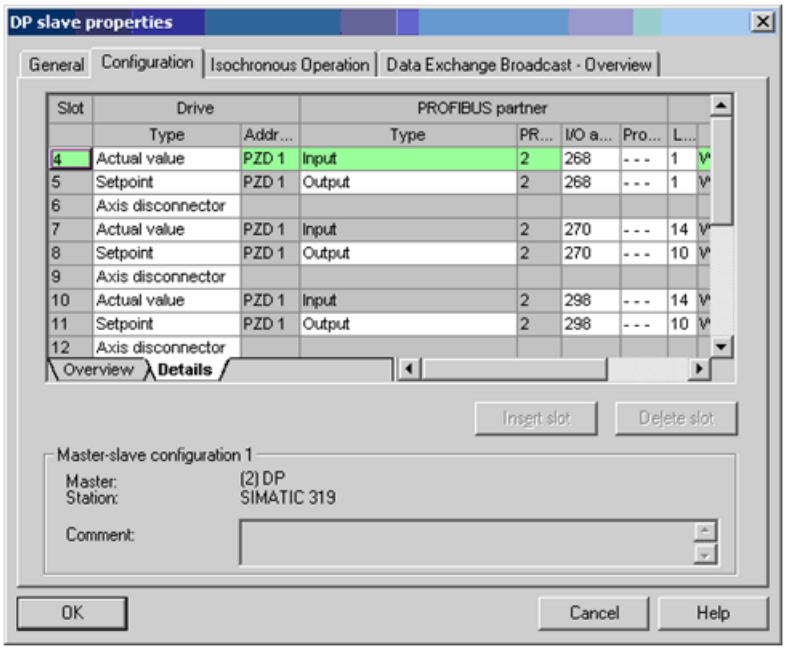


Figure A-13 Slave properties – details

The axis separator separates the objects in the telegram as follows:

- Slots 4 and 5: Object 1 –-> Active Infeed (A_INF)
- Slots 7 and 8: Object 2 –-> SERVO 1
- Slots 10 and 11: Object 3 –-> SERVO 2

etc.

A.1.2.2 Commissioning PROFIBUS

Interfaces and diagnostic LED

A PROFIBUS interface with LEDs and address switches is available as standard on the CU320-2 DP Control Unit.

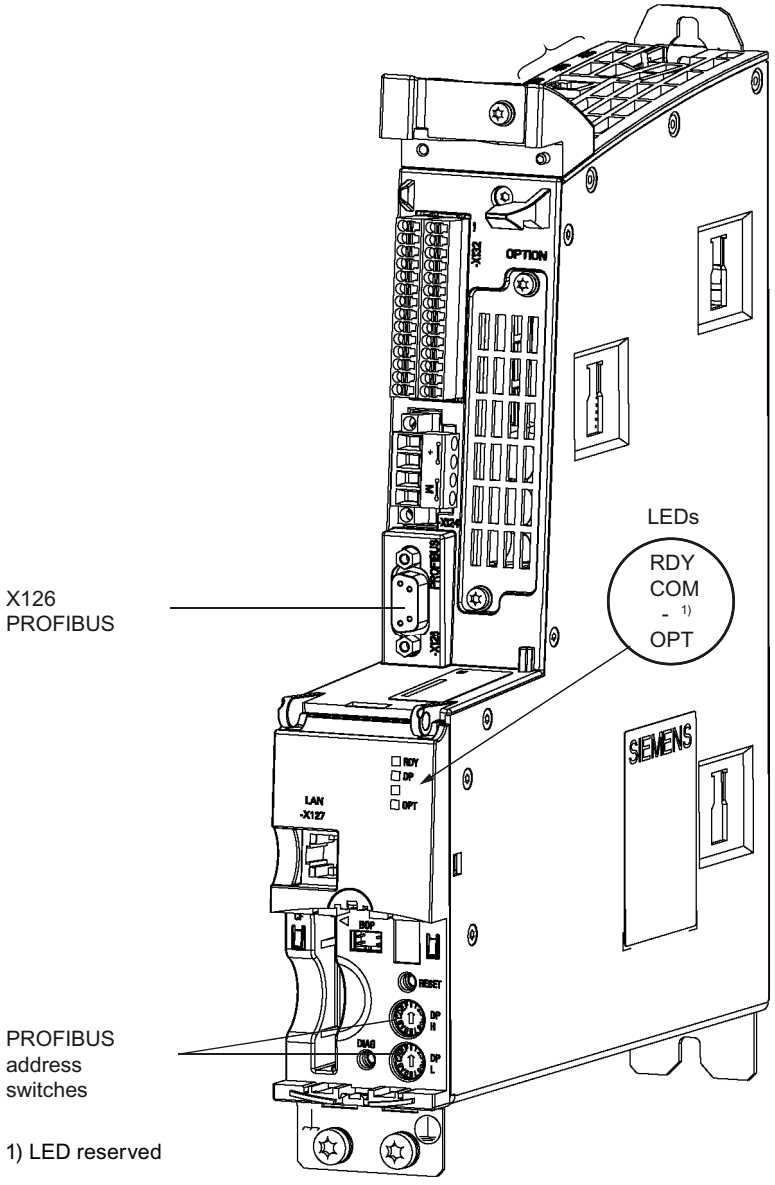


Figure A-14 Interfaces and diagnostic LED

- PROFIBUS interface
  The PROFIBUS is described in the "SINAMICS S120 Control Units and Supplementary System Components Manual".
- PROFIBUS diagnostic LED

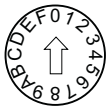
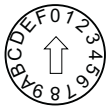
Note

A teleservice adapter can be connected to the PROFIBUS interface (X126) for remote diagnostics purposes.

PROFIBUS address switch

On the CU320-2 DP, the PROFIBUS address is set as a hexadecimal value via two rotary coding switches. You can set values from 0_{dec} (00_{hex}) to 127_{dec} ($7F_{hex}$). At the upper rotary coding switch (H) you set the hexadecimal value for 16^1 and at the lower rotary coding switch (L) you set the hexadecimal value for 16^0.

Table A-7 PROFIBUS address switch

Rotary coding switches	Significance	Examples		
		21_{dec}	**35_{dec}**	**126_{dec}**
		15_{hex}	**23_{hex}**	**$7E_{hex}$**
 DP H	$16^1 = 16$	1	2	7
 DP L	$16^0 = 1$	5	3	E

Setting the PROFIBUS address

Observe the properties of the rotary coding switch:

- The rotary coding switches used to set the PROFIBUS address are located beneath the cover.
- The factory setting for the rotary coding switches is 0_{dec} (00_{hex}).
- Address 126 is used for commissioning. Permitted PROFIBUS addresses are 1 ... 126.
- The currently set address of the rotary coding switch is displayed in parameter r2057.
- When several Control Units are connected to a PROFIBUS line, you set the addresses differently than for the factory setting. Each PROFIBUS address in a PROFIBUS line can only be assigned once. Either set the PROFIBUS address in absolute terms using the rotary coding switches – or selectively in parameter p0918. Each change made to the bus address is not effective until POWER ON.

Note

Only values from 1 to 126 ($7E_{hex}$) are valid for PROFIBUS addressing. If values above 127 are set, then the set value is interpreted as "0". If a value "0" or "127" is set, the value in parameter p0918 defines the PROFIBUS address.

There are two ways to set the PROFIBUS address:

1. Using the STARTER commissioning tool (parameter p0918)
   - To set the bus address for a PROFIBUS node using STARTER, first set the rotary code switches to 0_{dec} (00_{hex}) and/or 127_{dec} ($7F_{hex}$).
   - Then set the address to a value from 1 to 126 using parameter p0918.
2. Using the PROFIBUS address switches on the Control Unit
   - The address is set manually to values from 1 to 126 using the rotary coding switches. In this case, parameter p0918 is only used to read the address.

PROFIBUS interface in operation

Generic station description file

A generic station description file clearly and completely defines the properties of a PROFIBUS slave.

The SINAMICS S GSD file contains among other things standard telegrams, free telegrams and slave-to-slave telegrams for configuring slave-to-slave communication. With the aid of these telegram parts and an axis separator, a telegram for the drive unit must be composed for each drive object.

The GSD files can be found:

- On the Internet:
  PROFINET I/O (https://support.industry.siemens.com/cs/ww/en/view/49217480) (GSDML files)
  PROFIBUS DP (https://support.industry.siemens.com/cs/ww/en/view/49216293) (GSD files)
- On the CD/DVD of the Startdrive commissioning tool
- On the memory card in the directory:
  \\SIEMENS\SINAMICS\DATA\CFG\

The integration of a GSD file in HW Config is covered in the SIMATIC documentation. Suppliers of PROFIBUS components can provide their own bus configuration tool. The operation of the respective bus configuration tool is described in the relevant documentation.

Note for commissioning for VIK-NAMUR

To be able to operate a SINAMICS drive as a VIK-NAMUR drive, standard telegram 20 must be set and the VIK-NAMUR identification number activated via p2042 =1.

Device identification

Identification for individual slaves facilitates diagnostics and provides an overview of the nodes on the PROFIBUS.

The information for each slave is stored in the following CU-specific parameter:
r0964[0...6] device identification

Bus terminating resistor and shielding

Reliable data transmission via PROFIBUS depends, amongst other things, on the setting of the bus terminating resistors and the shielding of the PROFIBUS cables.

- Bus terminating resistor
  The bus terminating resistors in the PROFIBUS plugs must be set as follows:
  - First and last nodes in the line: Switch on terminating resistor
  - Other nodes in the line: Switch off terminating resistor
- Shielding of the PROFIBUS cables
  The cable shield must be connected in the plug through a large surface area at both ends (see SINAMICS S120 Control Units and Supplementary System Components Manual).

Commissioning PROFIBUS

Preconditions and assumptions for commissioning

	Requirement
PROFIBUS slave	• The PROFIBUS address to be set for the device application is known. • The telegram type for each drive object is known by the application.
PROFIBUS master	• The communication properties of the SINAMICS S120 slave must be available in the master (GSD file or Drive ES slave OM).

Commissioning steps (example with SIMATIC S7)

1. Set the PROFIBUS address on the slave.
2. Set the telegram type on the slave.

3. Perform the following in HW Config:
   – Connect the drive unit to PROFIBUS and assign the address.
   – Set the telegram type.
     The same telegram type as on the slave should be set for every drive object exchanging process data via PROFIBUS.
     The master can send more process data than the slave uses. A telegram with a larger number of PZDs than assigned for the SINAMICS drive object can be configured on the master.
     The PZDs not supplied by the drive object are filled with zeros.
     The setting "without PZD" can be defined on a node or object (e.g. infeed controlled via terminals).
4. Assign the I/O addresses according to the user program.

Diagnostics options

The standard slave diagnostics can be read online in the HW config.

SIMATIC HMI addressing

You can use a SIMATIC HMI as a PROFIBUS master (master class 2) to access SINAMICS directly. With respect to SIMATIC HMI, SINAMICS behaves like a SIMATIC S7. For accessing drive parameters, the following applies:

- Parameter number = data block number
- Parameter sub-index = bit 0 ... 9 of data block offset
- Drive object number = bit 10 ... 15 of data block offset

Pro Tool and WinCC flexible

The SIMATIC HMI can be configured flexibly with "Pro Tool" or "WinCC flexible".

The following specific settings for drives must be observed when configuration is carried out with Pro Tool or WinCC flexible.

Controllers: Protocol always "SIMATIC S7 - 300/400"

Table A-8 Additional parameters

Field	Value
Network parameter profile	DP
Network parameter baud rate	Any
Communication partner address	PROFIBUS address of the drive unit
Communication partner slot/rack	Don’t care, 0

Table A-9 Variables: "General" tab

Field	Value
Name	Any
Controller	Any
Type	Depending on the addressed parameter value, e.g.: INT: for integer 16 DINT: for integer 32 WORD: for unsigned 16 REAL: for float
Area	DB
DB (data block number)	Parameter number 1 ... 65535
DBB, DBW, DBD (data block offset)	Drive object No. and sub-index bit 15 ... 10: Drive object No. 0 ... 63 bit 9 ... 0: Sub-index 0 ... 1023 or expressed differently DBW = 1024 * drive object No. + sub-index
Length	Not activated
Acquisition cycle	Any
Number of elements	1
Decimal places	Any

Note

- You can operate a SIMATIC HMI together with a drive unit independently of an existing controller.
  A basic "point-to-point" connection can only be established between two nodes (devices).
- The "variable" HMI function can be used for drive units. Other functions cannot be used (e.g. "messages" or "recipes").
- Individual parameter values can be accessed. Entire arrays, descriptions, or texts cannot be accessed.

Monitoring telegram failure

When monitoring the telegram failure, SINAMICS differentiates between two cases:

- Telegram failure with a bus fault
- Telegram failure with a CPU stop

Telegram failure with a bus fault

- After a telegram failure and the additional monitoring time has elapsed (p2047), bit r2043.0 is set to "1" and alarm A01920 is output. Binector output r2043.0 can be used for a quick stop, for example.
- Once the delay time p2044 has elapsed, fault F01910 is output. Fault F01910 triggers fault response OFF2 (pulse inhibit) for the infeed and OFF3 (quick stop) for SERVO/VECTOR. If no OFF response is to be triggered, the fault response can be reparameterized accordingly.
- Fault F01910 can be acknowledged immediately. The drive can then be operated even without PROFIdrive.
- After telegram failure, bit r2043.0 is set to "1". Binector output r2043.0 can be used for a quick stop, for example.

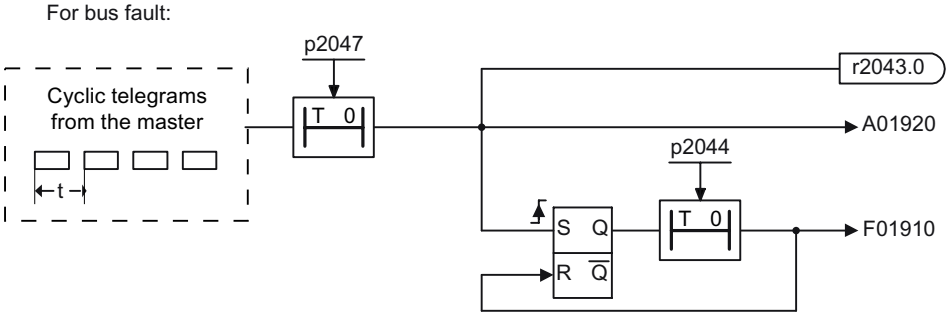


Figure A-15 Monitoring telegram failure with a bus fault

Telegram failure with a CPU stop

- Once the delay time p2044 has elapsed, fault F01910 is output. Fault F01910 triggers fault response OFF2 (pulse inhibit) for the infeed and OFF3 (quick stop) for SERVO/VECTOR. If no OFF response is to be triggered, the fault response can be reparameterized accordingly.
- Fault F01910 can be acknowledged immediately. The drive can then be operated even without PROFIdrive.

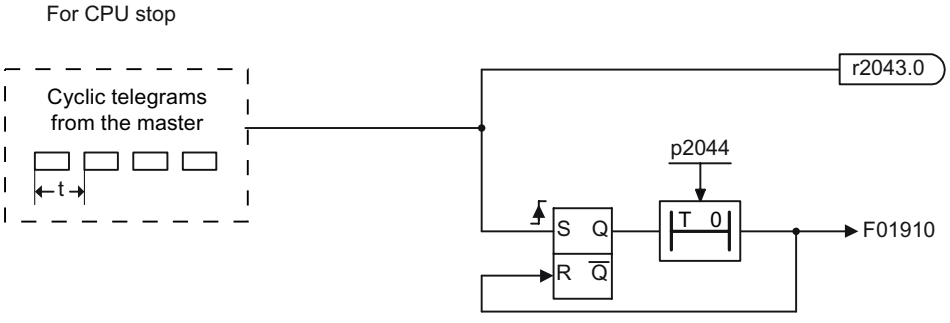


Figure A-16 Monitoring telegram failure for a CPU stop

Example: Quick stop at telegram failure

- Assumption
  - A drive unit with an Active Line Module and a Single Motor Module.
  - VECTOR mode is activated.
  - After a ramp-down time (p1135) of two seconds, the drive is at a standstill.
- Settings

CU	p2047	= 20 ms
A_INF	p2044	= 2 s
VECTOR	p2044	= 0 s

- Sequence
  - Following a telegram failure and once the additional monitoring time (p2047) has elapsed, binector output r2043.0 of drive object CU switches to "1".
  - At the same time, alarm A01920 is output for the A_INF drive objects and alarm A01920 and fault F01910 are output for VECTOR.
  - When F01910 is output, an OFF3 is triggered for the drive.
  - After a two-second delay time (p2044), fault F01910 is output on the infeed and triggers OFF2.

A.1.2.3 Motion Control with PROFIBUS

Motion control / isochronous drive coupling with PROFIBUS

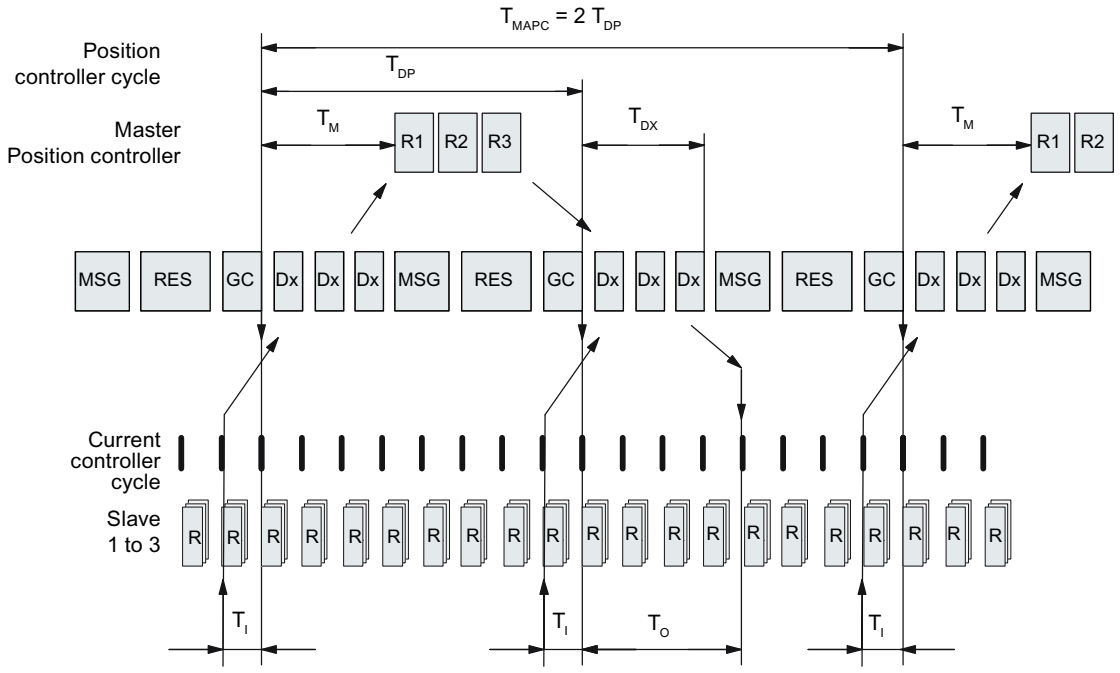


Figure A-17 Motion control / isochronous drive coupling with PROFIBUS, optimized cycle with $T_{MAPC} = 2 \cdot T_{DP}$

Sequence of data transfer to closed-loop control system

1. The actual position value G1_XACT1 is read into at time T_I before the start of each cycle and transferred to the master in the next cycle.
2. The closed-loop control of the master starts at time T_M after each position controller cycle and uses the transferred actual value in the telegram.
3. In the next cycle, the master forwards the calculated setpoints to the slaves. The speed setpoint command NSET_B is issued to the closed-loop control system at time T_O after the beginning of the cycle.

Time settings

Designations and descriptions for motion control

Table A-10 Time settings and meanings

Name	Limit value	Description
T_{BASE_DP}	250 µs	Time base for T_{DP}
T_{DP}	$T_{DP} \geq T_{DP\_MIN}$ $T_{DP\_MIN} \leq T_{DP} \leq T_{DP\_MAX}$	DP cycle time T_{DP} = Dx + MSG + RES + GC T_{DP} = multiple integer · T_{BASE_DP} T_{DP_MIN} = 1 ms T_{DP_MAX} = 32 ms
T_{MAPC}		Master application cycle time This is the time frame in which the master application generates new setpoints (e.g. in the position controller cycle). T_{MAPC} = integer multiple of T_{DP}
T_{BASE_IO}	125 µs	Time base for T_I, T_O
T_I	$T_{I\_MIN} \leq T_I < T_{DP}$	Time of actual value sensing This is the time at which the actual position value is captured before the start of each cycle. T_I = integer multiple of T_{BASE_IO} T_{I_MIN} corresponds to the longest current controller sampling time (p0115[0]) of a drive object (SERVO/VECTOR) in the drive unit, minimum 125 µs. Does not apply to vector U/f.
T_O	$T_{DX} + T_{O\_MIN} \leq T_O < T_{DP}$	Time of setpoint transfer This is the time at which the transferred setpoints (speed setpoint) are accepted by the closed-loop control system after the start of the cycle. T_O = integer multiple of T_{BASE_IO} T_{O_MIN} corresponds to the longest speed controller cycle (p0115[1]) of a drive object (SERVO/VECTOR) in the drive unit, minimum 125 µsec
T_{DX}	$T_{DX} < T_{DP}$	Data exchange time This is the time required within one cycle for transferring process data to all available slaves.
T_{PLL_W}	-	PLL window
T_{PLL_D}	-	PLL delay time
GC	-	Global Control Telegram (broadcast telegram)
Dx	-	Data_Exchange This service is used to implement user data exchange between master and slave 1 - n.
MSG	-	Acyclic service This service is used to implement user data exchange between master and slave 1 - n on an acyclic basis.
RES	-	Reserve: "Active pause" until the isochronous cycle has expired
R	-	Computation time, speed or position controller in the master or slave
T_M	-	Master time Start of closed-loop master control

Setting criteria for times

- Cycle (T_{DP})
  - T_{DP} must be set to the same value for all bus nodes.
  - $T_{DP} > T_{DX}$ and $T_{DP} > T_O$

  Note

  After T_{DP} has been changed on the PROFIBUS master, the drive system must be switched on (POWER ON) or parameter p0972 = 1 (reset drive unit) must be set.

- T_I and T_O
  - Setting the times in T_I and T_O as short as possible reduces the dead time in the position control loop.
  - $T_O > T_{DX} + T_{Omin}$
- Settings and tuning can be done using a tool (e.g. HW Config in SIMATIC S7).

Minimum times for reserves

Table A-11 Minimum times for reserves

Data	Time required [µs]
Basic load	300
Per slave	20
Per byte of user data	1.5
One additional class 2 master	500

Example: SINAMICS vector drives with SIMOTION D4x5 and/or CX modules

To determine which cycles in the SINAMICS drive unit will be set after a project has been downloaded, dependable cycle values should be initially set in HW Config.

The following settings and sequences are recommended:

1. T_{DP} = 3.0 ms (T_{DP} = DP cycle time)
2. $T_I = T_o$ = 1.5 ms (T_I = time of actual value acquisition, T_o = time of setpoint transfer)
3. T_{MAPC} = 6.0 ms (T_{MAPC} = master application cycle time)

After a successful download, all current and speed controller cycles are visible. These cycles can be optimized in HW Config if necessary.

The cycles are set in HW Config under the DP slave properties of the SINAMICS drive unit (slave, master e.g. SIMOTION D4x5) under the "Clock synchronization" tab.

User data integrity

User data integrity is verified in both transfer directions (master <––> slave) by a sign-of-life (4-bit counter).

The sign-of-life counters are incremented from 1 to 15 and then start again at an arbitrary value between 1 and 15.

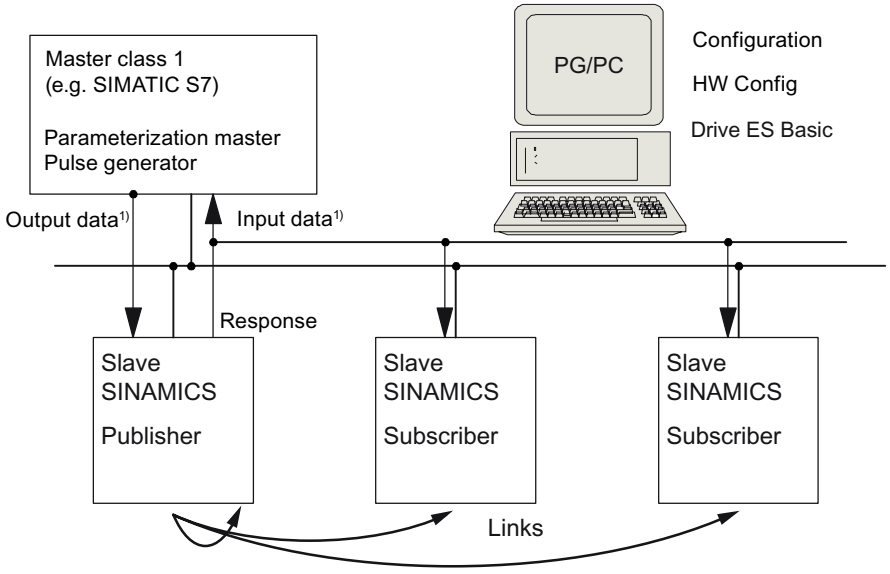
- Master sign-of-life
  - STW2.12 ... STW2.15 are used for the master sign-of-life.
  - The master sign-of-life counter is incremented on each master application cycle (T_{MAPC}).
  - The number of tolerated master sign-of-life errors in succession (of an isochronous motor) can be set via p0925
  - p0925 = 65535 deactivates sign-of-life monitoring on the slave.
  - Monitoring
    The master sign-of-life is monitored on the slave and any sign-of-life errors are evaluated accordingly.
    The maximum number of tolerated master sign-of-life errors can be set via p0925.
    If the number of tolerated sign-of-life errors in succession set in p0925 is exceeded, the response is as follows:
    – A corresponding message is output.
    – The value zero is output as the slave sign-of-life.
    – Synchronization with the master sign-of-life is started.
- Slave sign-of-life
  - ZSW2.12 ... ZSW2.15 are used for the slave sign-of-life.
  - The slave sign-of-life counter is incremented in each DP cycle (T_{DP}).

A.1.2.4 Slave-to-slave communication

For PROFIBUS DP, the master interrogates all of the slaves one after the other in a DP cycle. In this case, the master transfers its output data (setpoints) to the particular slave and receives as response the input data (actual values). Fast, distributed data transfer between drives (slaves) is possible using the "slave-to-slave communication" function without direct involvement from the master.

The following terms are used for the function described in this chapter:

- Slave-to-slave communication
- Data Exchange Broadcast (DXB.req)
- Slave-to-slave communication (is used in the following)



1) From the perspective of the Class 1 master

Figure A-18 Slave-to-slave communication with the publisher-subscriber model

Publisher

With the "slave-to-slave communication" function, at least one slave must act as the publisher.

The publisher is addressed by the master when the output data is transferred with a modified layer 2 function code (DXB.req). The publisher then sends its input data for the master with a broadcast telegram to all bus nodes.

Subscriber

The subscribers evaluate the broadcast telegrams, sent from the publishers, and use the data which has been received as setpoints. These setpoints of the publisher are used, in addition to the setpoints received from the master, corresponding to the configured telegram structure (p0922).

Links and taps

The links configured in the subscriber (connections to publisher) contain the following information:

- From which publisher is the input data received?
- What is the content of the input data?
- Where are the additional setpoints received?

Several taps are possible within a link. Several input data or input data areas, which are not associated with one another, can be used as setpoint via a tap.

Links on the drive unit itself are possible. For example, data in a Double Motor Module can be transferred from drive A to drive B. This internal link corresponds, as far as the timing is concerned, to a link via PROFIBUS.

Requirements

The following preconditions should be observed for the "slave-to-slave communication" function:

- STARTER as of Version 4.2

  Note

  Startdrive

  Please note that you still cannot use this function with Startdrive.

- Configuration:
  - Drive ES Basic, Drive ES SIMATIC or Drive ES PCS7 Version 5.3 SP3 or higher
  - Alternatively, using a GSD file
- Firmware as of Version 4.3
- The maximum number of process data per drive can be identified from the value in r2050 – minus the resources that have already been used
- A maximum of 16 links to publishers

Note

The "slave-to-slave communication" function is not available for the CU310-2 PN.

Applications

For example, the following applications can be implemented using the "slave-to-slave communication" function:

- Axis couplings (this is practical for isochronous mode)
- Specifying binector connections from another slave

Setpoint assignment in the subscriber

Information about setpoints

- Number of setpoint
  When bus communication is being established, the master signals the slave the number of setpoints (process data) to be transferred using the configuring telegram (ChkCfg).
- Contents of the setpoints
  The structure and contents of the data are determined using the local process data configuration for the "SINAMICS slave".
- Operation as "standard" slave
  The drive unit (slave) only receives its setpoints as output data from the master.
- Operation as subscriber
  These setpoints of the publisher are used, in addition to the setpoints received from the master, corresponding to the configured telegram structure (p0922).
  The slave is informed of the assignment via the parameterization and configuration telegram when bus communication is being established.

Activating/parameterizing slave-to-slave communication

The "slave-to-slave communication" function must be activated both in the publishers as well as in the subscribers, whereby only the subscriber is to be configured. The publisher is automatically activated during bus startup.

Activation in the publisher

The master is informed abut which slaves are to be addressed as publishers with a modified layer 2 function code (DXB req) via the configuration of the subscriber links.

The publisher then sends its input data not only to the master but also as a broadcast telegram to all bus nodes.

These settings are made automatically using the bus configuration tool (e.g. HW Config).

Activation in the subscriber

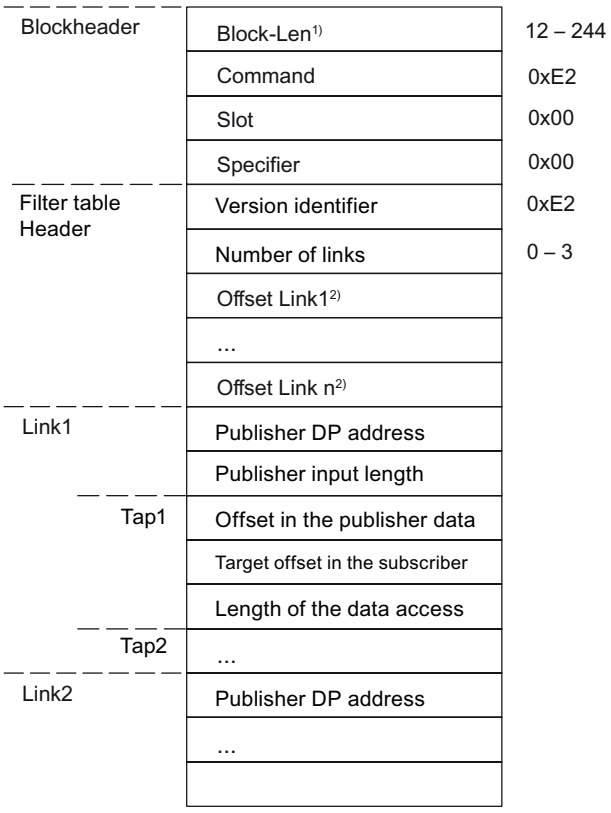
The slave, which is to be used as subscriber, requires a filter table. The slave must know which setpoints are received from the master and which are received from a publisher.

The filter table is created automatically via the bus configuration tool (e.g. HW Config).

The following diagram shows the information contained in the filter table.

Parameterizing telegram (SetPrm)

The filter table is transferred, as dedicated block from the master to the slave with the parameterizing telegram when a bus communication is established.



1) Specification in bytes
2) Calculated from Version ID

Figure A-19 Filter block in the parameterizing telegram (SetPrm)

Configuration telegram (ChkCfg)

Using the configuration telegram, a slave knows how many setpoints are to be received from the master and how many actual values are to be sent to the master.

For slave-to-slave communication, a special space ID is required for each tap. The PROFIBUS configuration tool (e.g. HW Config) generates this ID. The ID is then transferred with the ChkCfg into the drive devices that operate as subscribers.

Commissioning PROFIBUS slave-to-slave communication

The commissioning of slave-to-slave communication between two SINAMICS drive devices using the additional Drive ES package is described below in an example.

Settings in HW Config

Based on the example of the project below, the settings in HW Config are described when using standard telegrams.

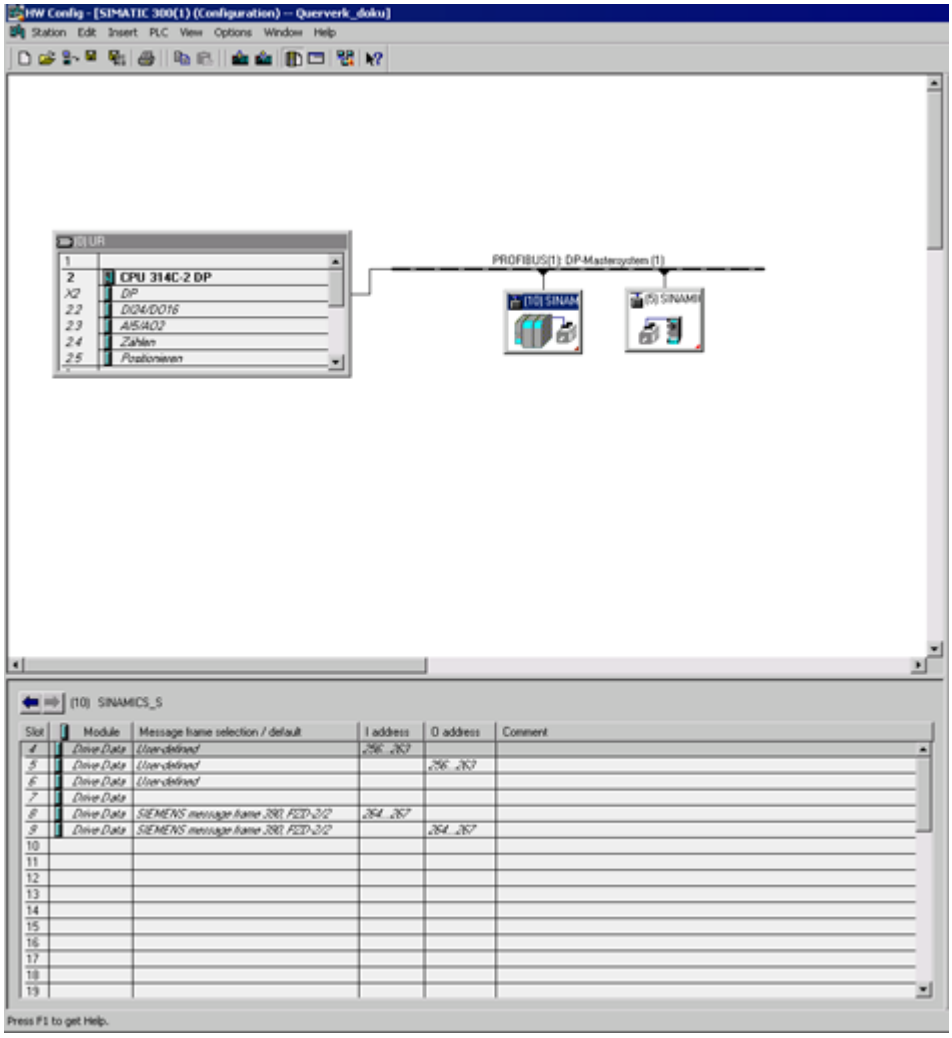


Figure A-20 Example project of a PROFIBUS network in HW Config

Procedure

1. You have generated a project, e.g. with SIMATIC Manager and HW Config. In the project example, you defined a CPU 314 controller as master and 2 SINAMICS S120 Control Units as slaves. Of the slaves, one CU310-2 DP is the publisher and one CU320-2 DP the subscriber.
2. Select the CU320-2 DP Control Unit as slave.

3. Via its properties dialog in the overview, configure the telegram for the connected drive object.

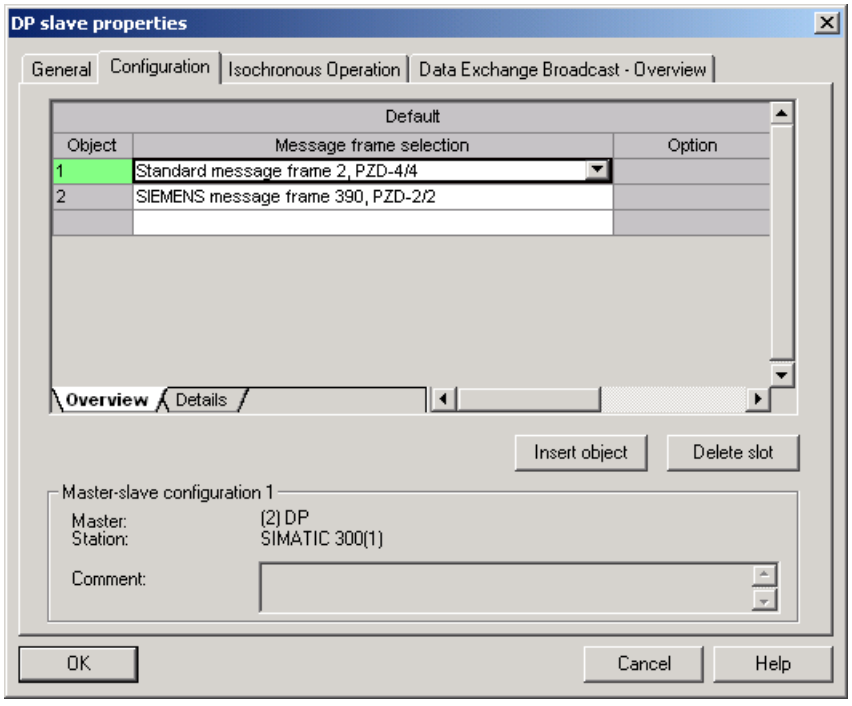


Figure A-21 Telegram selection for drive object

4. Then switch to the detailed view.
   - Slots 4/5 contain the actual and setpoint values for the first drive object, e.g. SERVO.
   - Slots 7/8 contain the telegram components for the actual values and setpoints for the second drive object, e.g. CU310-2 DP.

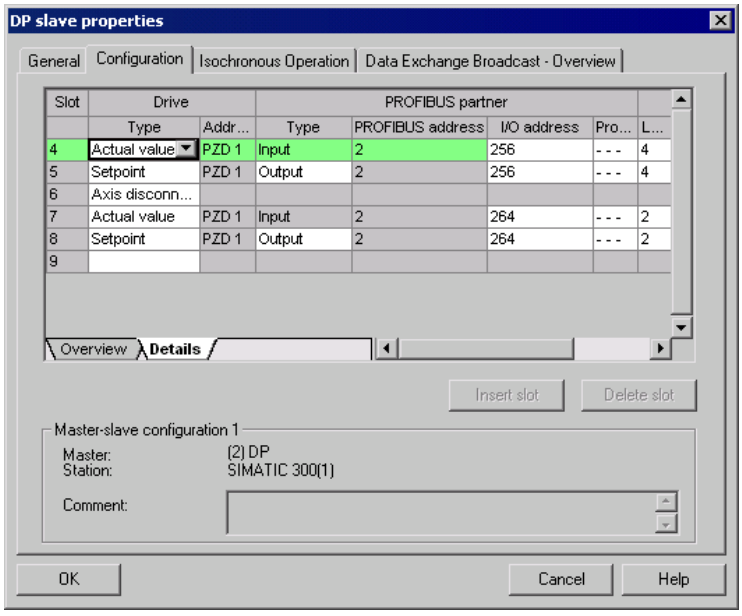


Figure A-22 Detail view of slave configuration

5. Create an additional setpoint slot 6 for the first drive object using the "Insert slot" button behind the existing setpoint slot 5.

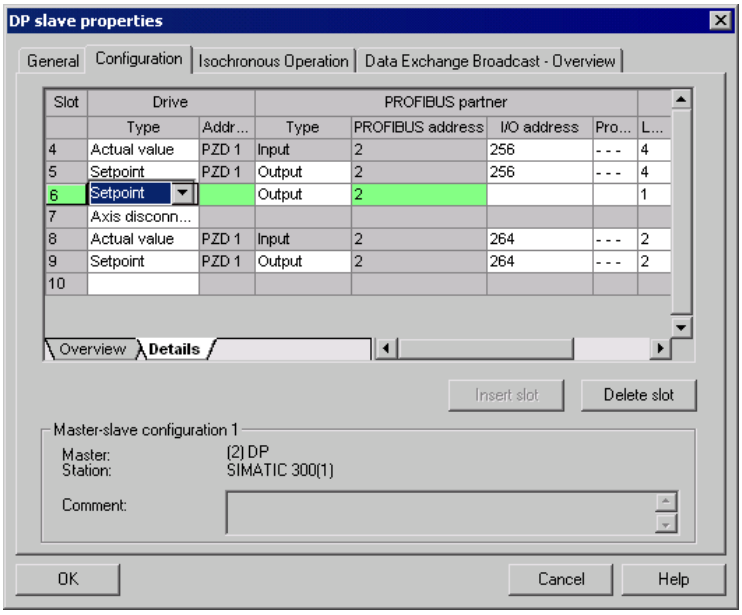


Figure A-23 Insert new slot

6. Under the "PROFIBUS Partner" column, change the new setpoint slot 6 from an "output" type to a "slave-to-slave communication" type.
7. In the first column, select the PROFIBUS DP address of the publisher, in this example "5". All PROFIBUS DP slaves are listed here, for which actual value data can be retrieved. It also provides the possibility of sharing data via slave-to-slave communication within the same drive device.

8. The "I/O address" column displays the start address for every drive object.
   Select the start address of the data of the drive object to be read. In the example, "268" is proposed.
   If the complete data of the publisher is not to be read, set this using the "Length" column.
   Alternatively, you can shift the start address of the access, so that the required data can be read out from the center section of the telegram component of the drive object.

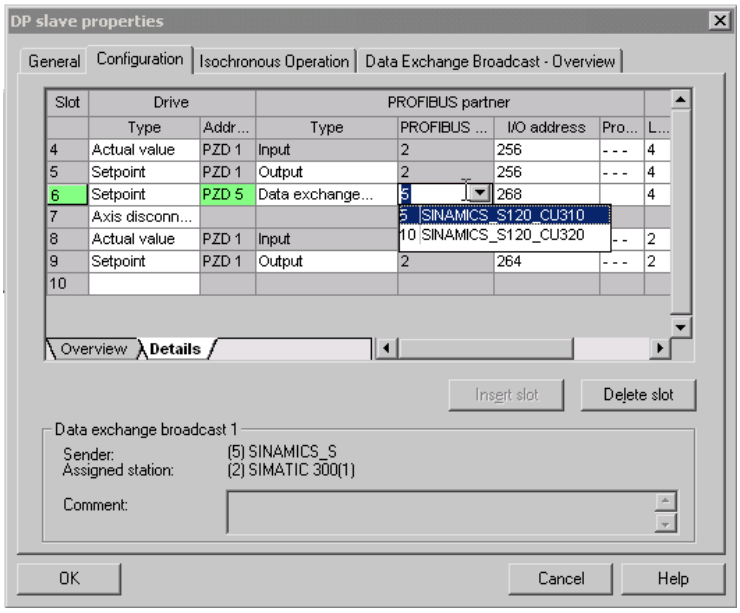


Figure A-24 Configuring the slave-to-slave communication nodes

9. Click the "Slave-to-slave communication overview" tab.
   The configured slave-to-slave communication relationships are shown here which correspond to the current status of the configuration in HW Config.

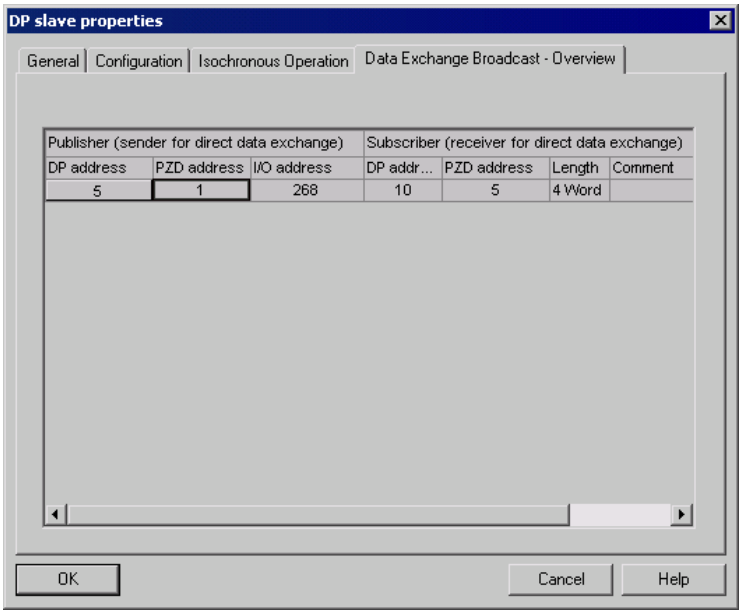


Figure A-25 Slave-to-slave communication - overview

After the slave-to-slave communication link has been created, instead of showing "Standard telegram 2" for the drive object, "User-defined" appears in the configuration overview under telegram selection.

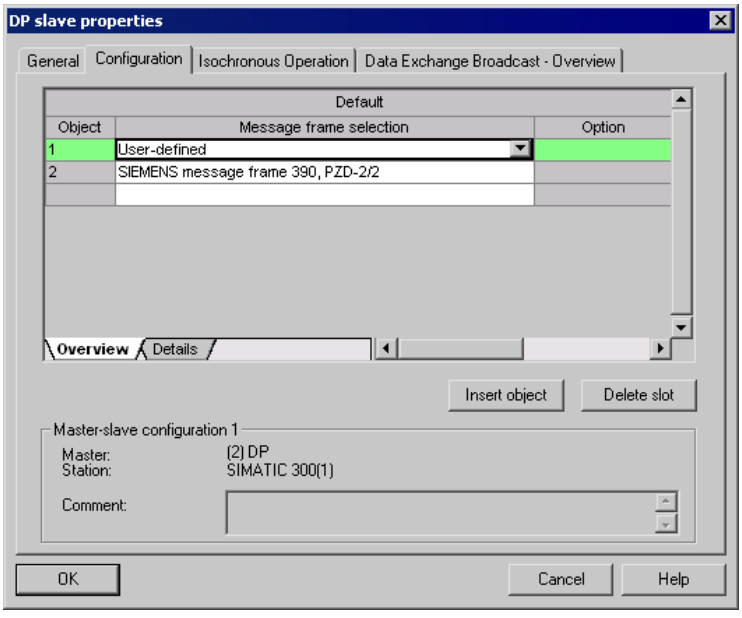


Figure A-26 Telegram assignment for slave-to-slave communication

The details after creation of the slave-to-slave communication link for a drive object of the drive device are as follows:

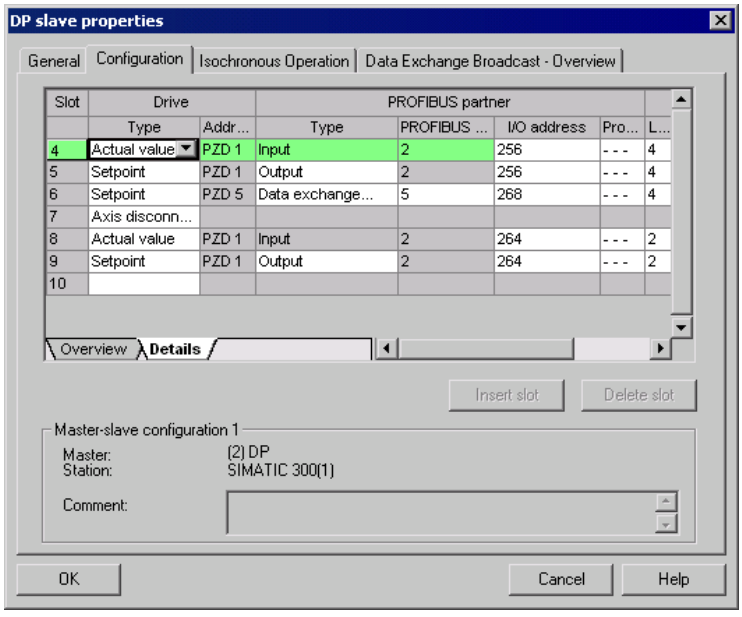


Figure A-27 Details after the creation of the slave-to-slave communication link

10. You should therefore adjust the telegrams for each drive object of the selected drive device that is to participate actively in slave-to-slave communication.

Automatic identification in Startdrive

The settings made in HW Config for the slave-to-slave telegrams are automatically detected by Startdrive. A telegram extension is not required in Startdrive.

Diagnosing PROFIBUS slave-to-slave communication

Since the PROFIBUS slave-to-slave communication is implemented on the basis of a broadcast telegram, only the subscriber can detect connection or data faults, e.g. via the publisher data length (see "Configuration telegram").

The publisher can only detect and report an interruption of the cyclic connection to the DP master (A01920, F01910). The broadcast telegram to the subscriber will not provide any feedback. A fault of a subscriber must be fed back via slave-to-slave communication. In case of a "master drive" 1:n, however, the limited quantity framework (see "Links and requests") should be observed. It is not possible to have n subscribers report their status via slave-to-slave communication directly to the "master drive" (publisher).

Diagnostics can be performed using the diagnostic parameters r2075 ("Receive PROFIBUS diagnostics telegram offset PZD") and r2076 ("Send PROFIBUS diagnostics telegram offset PZD"). The parameter r2074 ("PROFIBUS diagnostics, receive bus address PZD") displays the DP address of the setpoint source of the respective PZD.

r2074 and r2075 enable the source of a slave-to-slave communication relationship to be verified in the subscriber.

Note

The subscribers do not monitor the existence of an isochronous publisher sign-of-life.

Faults and alarms with PROFIBUS slave-to-slave communication

The alarm A01945 signals that the connection to a least one publisher of the drive device is missing or has failed. Any interruption to the publisher is also reported by the fault F01946 at the affected drive object. A failure of the publisher only impacts the respective drive objects.

More detailed information on the messages can be found in the SINAMICS S120/S150 List Manual.

A.1.2.5 Messages via diagnostics channels

Overview

Messages are not just able to be displayed via the Startdrive commissioning tools. After the activation of a diagnostic function, the messages are also transferred to the higher-level controller via the standardized PROFIdrive fault classes. The messages are evaluated there or forwarded for convenient display to the corresponding user interfaces (SIMATIC HMI, TIA Portal, etc.).

In this way, problems or faults can be located immediately regardless of the tool currently being used, and then corrected immediately.

Also note the general information on the diagnostics channels in Chapter Diagnostics channels (Page 98).

Activating the diagnostic function

The diagnostics function is activated or deactivated via the parameterization of the relevant configuration tool (HW Config, TIA Portal, etc.).

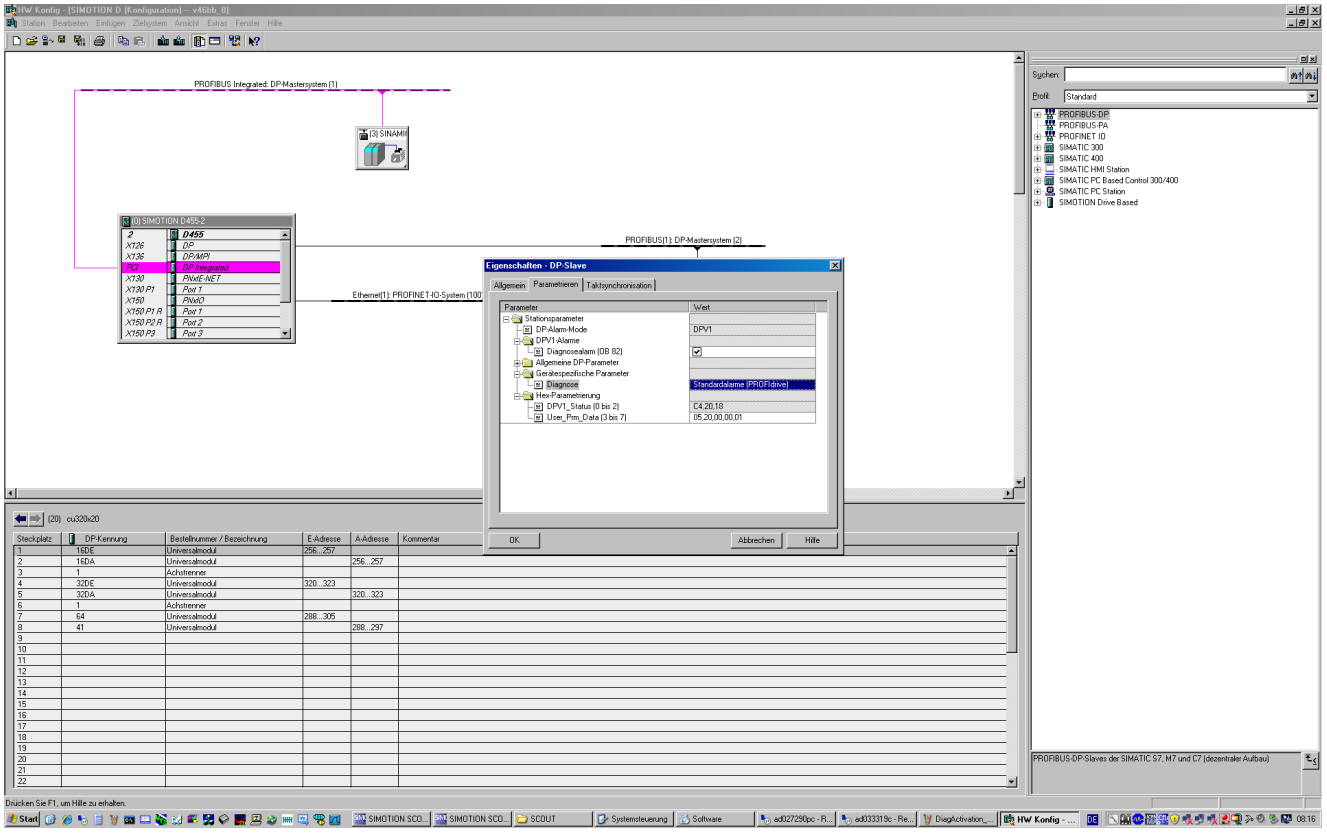


Figure A-28 Activation of PROFIBUS

The following parameter assignments are possible:

Setting	Code for parameter assignment
Inactive	0
PROFIdrive error classes	1

When establishing the communication between SINAMICS and a master, the activated diagnostics mode of this controller is first transferred to the drive. With activated diagnostics, SINAMICS first transfers all pending messages to the master. Symmetrically, all currently active messages in the master are deleted by SINAMICS when closing the communication connection.

Messages

The message texts are described in detail in the SINAMICS S120/S150 List Manual, Section 4.1.2 "Explanations on the list of faults and alarms". A current list of the message texts can be found in the "Message classes and coding of different diagnostics interfaces" table.

A.1.3 Communication via PROFINET IO

A.1.3.1 General information about PROFINET IO

PROFINET IO is an open Industrial Ethernet standard for a wide range of production and process automation applications. PROFINET IO is based on Industrial Ethernet and observes TCP/IP and IT standards.

Deterministic signal processing in real time is important in industrial networks. PROFINET IO satisfies these requirements.

The international standard IEC 61158 ensures open, multi-vendor systems:

PROFINET IO is tuned for high-speed, time-critical data transfers at field level.

PROFINET IO

Within the context of Totally Integrated Automation (TIA), PROFINET IO is the systematic development of the following systems:

- PROFIBUS DP, the established fieldbus,
- Industrial Ethernet, the communications bus for the cell level.

Experience gained from both systems was integrated into PROFINET IO. An Ethernet-based automation standard defined by PROFIBUS International (PROFIBUS user organization), PROFINET IO is a manufacturer-independent communication and engineering model.

PROFINET IO defines every aspect of the data exchange between IO controllers (devices with so-called "master functionality" and the IO devices (devices with so-called "slave functionality") as well as carrying out parameterization and diagnostics. A PROFINET IO system is configured in virtually the same way as a PROFIBUS system.

A PROFINET IO system is assembled from the following devices:

- An IO controller controls automation tasks.
- An IO device is controlled and monitored by an IO controller. An IO device can consist of several modules and submodules.
- An IO supervisor is an engineering tool, typically based on a PC, to configure e and diagnose the individual IO devices (drive units).

IO devices: Drive units with PROFINET interface

- SINAMICS S120 with CU320-2 DP and inserted CBE20 (X1400)
- SINAMICS S120 with CU320-2 PN
- SINAMICS S120 with CU310-2 PN

Cyclic communication using PROFINET IO with IRT or using RT is possible on all drive units equipped with a PROFINET interface. This means that error-free communication using other standard protocols is guaranteed within the same network.

Note

PROFINET for drive technology is standardized and described in the following document:

PROFIBUS profile PROFIdrive - Profile Drive Technology

PROFIBUS User Organization e. V.

Haid-und-Neu-Straße 7

D-76131 Karlsruhe

You can obtain the current version from "PROFIBUS and PROFINET International (PI) (https://www.profibus.com/download/profidrive-profile-drive-technology/)".

Order no. 3.172, spec. Section 6

- IEC 61800-7

Note

For CU320-2 DP with inserted CBE20 (X1400), the cyclic PZD channel for PROFIBUS DP is deactivated. When setting parameter p8839 = 1, the PZD channel can be reactivated (see Section "Parallel operation of communication interfaces (Page 83)").

Real-time (RT) and isochronous real-time (IRT) communication

Real-time communication

When communication takes place via TCP/IP, the resultant transmission times may be too long and not defined to meet the production automation requirements. When communicating time-critical IO user data, PROFINET IO therefore uses its own real-time channel, rather than TCP/IP.

Real time means that a system processes external events over a defined period.

Determinism

Determinism means that a system will react in a predictable ("deterministic") manner.
With PROFINET IO with IRT, it is possible to precisely determine (predict) transmission times.

PROFINET IO with RT (Real Time)

Real-time data is treated with a higher priority than TCP(UDP)/IP data. Transmission of time-critical data takes place at guaranteed time intervals. RT communication provides the basis for data exchange with PROFINET IO.

PROFINET IO with IRT (Isochronous Real Time)

Isochronous real time: Real time property of PROFINET IO where IRT telegrams are transferred deterministically via planned communication paths in a defined sequence to achieve the best possible synchronism and performance between the IO controller and IO device (drive unit). IRT is also known as time-scheduled communication whereby knowledge about the network structure (topology) is utilized. IRT requires special network components that support planned data transfer.

SINAMICS cycle times of minimum 250 µs (onboard) / 500 µs (CBE20) and a jitter accuracy of less than 1 µs can be achieved when this transmission method is implemented.

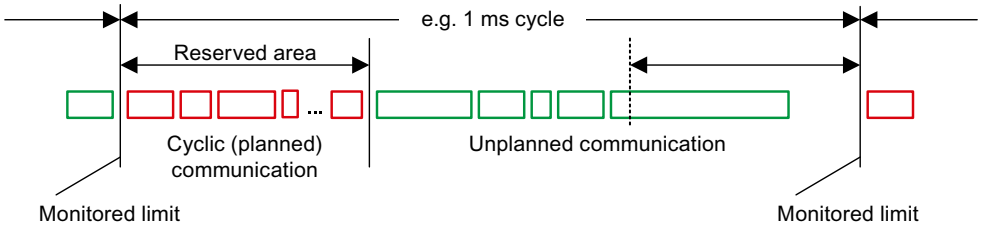


Figure A-29 Bandwidth distribution/reservation, PROFINET IO

Addresses

MAC address

Every Ethernet and therefore every PROFINET interface is assigned a worldwide unique device identifier in the factory. This 6-byte long device identifier is the MAC address. The MAC address is divided up as follows:

- Three bytes for the manufacturer's ID
- Three bytes for the device identifier (consecutive number)

The MAC address is printed on a label (CBE20) or specified on the type plate (CU320-2 PN and CU310-2 PN), e.g.: 08-00-06-6B-80-C0.

The Control Units CU320-2 PN and CU310-2 PN have two integrated interfaces:

- One Ethernet interface
- One PROFINET interface with two ports

The MAC addresses of the Ethernet and PROFINET interfaces are stamped on the type plate.

IP address

The TCP/IP protocol is a prerequisite for establishing a connection and parameterization. To allow a PROFINET device to be addressed as a node on Industrial Ethernet, this device requires a unique IP address in the network. The IP address is made up of 4 decimal numbers with a range of values from 0 through 255. The decimal numbers are separated by a decimal point. The IP address comprises:

- The address of the node (also called host or network node)
- The address of the (sub) network

IP address assignment

The IP addresses of IO devices can be assigned by the IO controller and always have the same subnet mask as the IO controller. In this case, the IP address is not stored permanently. The IP address entry is lost after POWER ON/OFF. The IP address can be assigned retentively via the Startdrive function "Accessible nodes" (see SINAMICS S120 Commissioning Manual with Startdrive).

This function can also be performed with HW Config of STEP 7. The function is called "Edit Ethernet node" here.

Note

IP addresses of the onboard interfaces

It is not permissible that the IP address band of the Ethernet interface and the PROFINET interface are the same. The factory setting of the IP address of the Ethernet interface X127 is 169.254.11.22; the subnet mask is 255.255.0.0.

Note

If the network is part of an existing Ethernet company network, obtain the information (IP address) from your network administrator.

Notes regarding interface X127 LAN (Ethernet)

Note

Use

Ethernet interface X127 is intended for commissioning and diagnostics, which means that it must always be accessible (e.g. for service).

Further, the following restrictions apply to X127:

- Only local access is possible
- No networking - or only local networking in a closed and locked electrical cabinet permissible

If it is necessary to remotely access the electrical cabinet, then additional security measures must be applied so that misuse through sabotage, unqualified data manipulation and intercepting confidential data is completely ruled out (also see "Industrial Security (Page 17)").

Device name (NameOfStation)

When it is shipped, an IO device does not have a device name. An IO device can only be addressed by an IO controller, for example, for the transfer of project engineering data (including the IP address) during startup or for user data exchange in cyclic operation, after it has been assigned a device name with the IO supervisor.

Note

The device name must be retentively saved – either with Startdrive or with the hardware configuration from STEP 7.

Note

Address information for interfaces

The address data for the corresponding interfaces can be entered in Startdrive in the expert list using the following parameters:

- X127 Ethernet interfaces:
  Parameters p8901, p8902, and p8903
- Internal PROFINET interfaces X150 P1 and P2:
  Parameters p8921, p8922 and p8923
- Interfaces of the optional CBE20 module (X1400):
  Parameters p8941, p8942 and p8943

Activating the interface configuration and saving it in non-volatile memory

To activate the interface configuration and save it in non-volatile memory, use the following parameter settings:

- X127 Ethernet interfaces: p8905 = 2
- Internal PROFINET interfaces X150 P1 and P2: p8925 = 2
- Interfaces of the optional CBE20 module (X1400): p8945 = 2

Replacing the CU320-2 DP/PN and CU310-2 PN Control Units (IO device)

If the IP address and device name are stored in non-volatile memory, this data is also forwarded with the memory card of the Control Unit. The memory card allows module exchange without an IO supervisor when a fault occurs in a PROFINET device.

If a complete Control Unit needs to be replaced due to a device or module defect, the new Control Unit automatically parameterizes and configures using the data on the memory card. Following this, cyclic exchange of user data is restarted.

Dynamic IP address assignment

In those cases in which the PROFINET interface is not used for the IO communication, it is possible to generate an IP address centrally using a DHCP (DHCP = Dynamic Host Configuration Protocol) server. The following requirements must be satisfied to do this:

- At least one DHCP server must be active.
- The PG/PC and the SINAMICS devices must be connected to the same physical Ethernet subnet.

Note

DHCP is not supported together with PROFINET. No cyclical connection is established for an activated DHCP. It is therefore recommended that DHCP not be used within PROFINET networks!

The DHCP address assignment can be set from the SIMATIC Manager or using SINAMICS parameters.

Setting the DHCP address assignment with SIMATIC Manager (STEP 7)

1. Call the "Target system > Edit Ethernet node" menu path in the SIMATIC Manager.
2. Click the "Search" button in the "Ethernet nodes" area.
3. Select the desired SINAMICS device.
   You can now specify in the "Edit Ethernet nodes" configuration dialog that a dynamic IP address will be generated via a DHCP server. The IP address can be identified in two ways:
   – MAC address
   – Device name (name of station)

   The "MAC address" option has the disadvantage that the MAC addresses are no longer correct after a device has been replaced.
4. Click the "Obtain the IP address from a DHCP server" option in the dialog to activate.
5. Activate either the "MAC address" or the "Device name" option in the "Identified via" area.
6. Click "Assign IP configuration".
   The IP address is then taken from the DHCP server. The SINAMICS device uses the associated setting after a POWER ON to obtain a new IP address from the DHCP server.

Setting the DHCP address assignment with SINAMICS parameters

As an alternative to the address assignment by the SIMATIC Manager, the DHCP address assignment can also be initiated using SINAMICS parameters. In this case, the Control Unit always fetches the IP address from a DHCP server after each POWER ON. You can make the settings using Startdrive "Parameter list":

1. Activate the DHCP address assignment using one of the following settings (where the values 2 and 3 mean "MAC address" and "Device name", respectively):
   - For Ethernet onboard (X127): p8904 = 2 or 3
   - For PROFINET onboard: p8924 = 2 or 3
   - For CBE20 (X1400): p8944 = 2 or 3

   The DHCP server now assigns temporarily an IP address.
2. You can now activate the interface configuration (value of 1) or activate and save retentively (value of 2). Make one of the following settings:
   - For Ethernet onboard (X127): p8905 = 1 or 2
   - For PROFINET onboard: p8925 = 1 or 2 (applies only to SINAMICS S120 devices)
   - For CBE20 (X1400): p8945 = 2
     Direct activation is not possible for the CBE20. The configuration can only be saved. The setting then becomes automatically active for the next POWER ON.

DCP flashing

This function is used to check the correct assignment to a module and its interfaces. This function is supported by a CU310-2 PN and a CU320-2 DP/PN with inserted CBE20. The function can also be used without CBE20 in a CU320-2 PN.

Activating DCP flashing:

1. In HW Config or the STEP 7 Manager, select the menu item "Target system > Ethernet > Edit Ethernet node".
   The "Edit Ethernet Node" dialog box opens.
2. Click the "Browse" button.
   The "Browse Network" dialog box opens and displays the connected nodes.
3. Select the CU310-2 PN or the CU320-2 DP with inserted CBE20 as node.
   The "DCP flashing" function is then activated via the "Flash" button.

The DCP flashing will be effective on the RDY LED (READY LED 2 Hz, green/orange or red/orange) on the CU310-2 PN/CU320-2 DP.

The LED will continue to flash as long as the dialog is open. When the dialog box is closed, the LED automatically goes dark. The function is available from STEP 7 V5.3 SP1 and higher via Ethernet or via Startdrive.

Data transfer

Properties

The PROFINET interface on a drive unit supports the simultaneous operation of:

- IRT – Isochronous Real Time Ethernet
- RT – Real Time Ethernet
- Standard Ethernet services (TCP/IP, LLDP, UDP and DCP)

PROFIdrive telegram for cyclic data transmission, acyclic services

PROFIdrive telegrams are available for implementing cyclic communication via PROFINET IO (see chapter "Communication according to PROFIdrive", Cyclic communication (Page 72)).

Telegrams to send and receive process data are available for each drive object of a drive unit with cyclic process data exchange.
In addition to cyclic data transfer, acyclic services can also be used for parameterizing and configuring the drive unit. These acyclic services can be utilized by the IO supervisor or IO controller.

Sequence of drive objects in the telegram

On the drive side, the sequence of drive objects in the telegram is displayed via a list in p0978[0...24] where it can also be changed.

Using the Startdrive commissioning tool you can display the sequence of drive objects for a commissioned drive system in the project navigator under "Drive unit" **>** "Communication" > "Telegram configuration".

When you create the configuration on the controller side (e.g. HW Config), the process-data-capable drive objects for the application are added to the telegram in the sequence shown (see above).

The following drive objects can exchange process data:

- Active Infeed (A_INF)
- Basic Infeed (B_INF)
- Control Unit (CU_S)
- ENC
- Smart Infeed (S_INF)
- SERVO
- VECTOR
- Terminal Board 30 (TB30)
- Terminal Module 15 (TM15)
- Terminal Module 31 (TM31)
- Terminal Module 41 (TM41)
- Terminal Module 120 (TM120)
- Terminal Module 150 (TM150)

Note

The sequence of drive objects in HW Config must be the same as that in the drive (p0978).

Drive objects after the first zero in p0978 must not be configured in the HW Config.

The structure of the telegram depends on the drive objects taken into account during configuration. Configurations are permitted that do not take into account all of the drive objects that are present in the drive system.

Example:

The following configurations are possible:

- Configuration with SERVO, SERVO, SERVO
- Configuration with A_INF, SERVO, SERVO, SERVO, TB30
- ...

Communication channels for PROFINET

PROFINET connection channels

- A Control Unit has an integrated Ethernet interface (X127).
- The PROFINET versions CU320-2 PN and CU310-2 PN each have a PROFINET interface (X150) with two onboard ports: P1 and P2
- A CU320-2 PN or a CU310-2 PN Control Unit can simultaneously establish a total of eight acyclic connections (e.g. S7) via the integrated PROFINET interfaces.

Notes regarding interface X127 LAN (Ethernet)

Note

Use

Ethernet interface X127 is intended for commissioning and diagnostics, which means that it must always be accessible (e.g. for service).

Further, the following restrictions apply to X127:

- Only local access is possible
- No networking - or only local networking in a closed and locked electrical cabinet permissible

If it is necessary to remotely access the electrical cabinet, then additional security measures must be applied so that misuse through sabotage, unqualified data manipulation and intercepting confidential data is completely ruled out (also see "Industrial Security (Page 17)").

Control Unit with CBE20

A Communication Board can be optionally inserted in the CU320-2 PN/DP Control Unit:

- The CBE20 Communication Board (X1400) is a PROFINET switch with 4 additional PROFINET ports.

Notes

Note

PROFINET routing

Routing is not possible between the onboard interfaces X127 and X150 – or between the onboard interfaces of the Control Unit 320-2 PN and an inserted CBE20 (X1400).

Note

PROFINET interfaces on the CU320-2 PN with CBE20

The integrated PROFINET interface of the CU320-2 PN is independent of the optionally inserted CBE20 module. The two PROFINET interfaces are not connected with each other. Routing is not possible between the two PROFINET interfaces.

Note

Ring topology

When connecting the ports, it must be ensured that for standard applications a ring topology is not created. Additional information on ring topologies can be found in Section Media redundancy (Page 175).

Note

Support for the medium-dependent interface auto-MDI(X)

- The Ethernet interface does not support auto-MDI(X). If the LAN interface of the communication partner also cannot handle auto-MDI(X), then a crossover cable must be used to establish the connection.
- The PROFINET interfaces support Auto MDI(X). It is therefore possible to use both crossed and uncrossed cables to connect the devices.
- The CBE20 Communication Board also supports auto-MDI(X). It is therefore possible to use both crossed and uncrossed cables to connect the devices.

Overview of important parameters

Ethernet interface

- p8900[0...239] IE Name of Station
- p8901[0...3] IE IP Address
- p8902[0...3] IE Default Gateway
- p8903[0...3] IE Subnet Mask
- p8904 IE DHCP Mode
- p8905 IE Interface Configuration
- r8910[0...239] IE Name of Station actual
- r8911[0...3] IE IP Address actual
- r8912[0...3] IE Default Gateway actual

- r8913[0...3] IE Subnet Mask actual
- r8915[0...5] IE MAC Address

Integrated PROFINET interface

- p8920[0...239] PN name of station
- p8921[0...3] PN IP address
- p8922[0...3] PN default gateway
- p8923[0...3] PN Subnet Mask
- p8924 PN DHCP mode
- p8925 PN interfaces configuration
- r8930[0...239] PN Name of Station actual
- r8931[0...3] PN IP Address actual
- r8932[0...3] PN Default Gateway actual
- r8933[0...3] PN Subnet Mask actual
- r8935[0...5] PN MAC Address
- r8936[0...1] PN cyclic connection state
- r8937[0...5] PN diagnostics
- r61000[0...239] PROFINET name of station
- r61001[0...3] PROFINET IP of station

CBE20

- p8940[0...239] CBE2x Name of Station
- p8941[0...3] CBE2x IP address
- p8942[0...3] CBE2x Default Gateway
- p8943[0...3] CBE2x Subnet Mask
- p8944 CBE2x DHCP mode
- p8945 CBE2x interfaces configuration
- r8950[0...239] CBE2x Name of Station actual
- r8951[0...3] CBE2x IP address actual
- r8952[0...3] CBE2x Default Gateway actual
- r8953[0...3] CBE2x Subnet Mask actual
- r8954 CBE2x DHCP Mode actual
- r8955[0...5] CBE2x MAC address
- r8959 CBE2x DAP ID
- r61000[0...239] PROFINET name of station
- r61001[0...3] PROFINET IP of station

A.1.3.2 RT classes for PROFINET IO

PROFINET IO is a scalable realtime communication system based on Ethernet technology. The scalable approach is expressed with three realtime classes.

RT

RT communication is based on standard Ethernet. The data is transferred via prioritized Ethernet telegrams. As standard Ethernet does not support any synchronization mechanisms, isochronous operation is not possible with PROFINET IO with RT.

The real update cycle in which cyclic data is exchanged depends on the bus load, the devices used and the quantity framework of the I/O data. The update cycle is a multiple of the send cycle.

IRT

Two options are available with this RT class:

- IRT "high flexibility"
- IRT "high performance"

The real-time classes IRT "high flexibility" and IRT "high performance" can be selected as options in the synchronization settings configuration area of HW Config. In the description below, both these classes are simply referred to as "IRT".

Software preconditions for configuring IRT:

- STEP 7 5.4 SP4 (HW Config)

Note

For further information about configuring the PROFINET interface for the I/O controller and I/O device, please refer to the following document: SIMOTION SCOUT Communication System Manual.

IRT "high flexibility"

The telegrams are sent cyclically in a deterministic cycle (Isochronous Real Time). The telegrams are exchanged in a bandwidth reserved by the hardware. One IRT time interval and one standard Ethernet time interval are created for each cycle.

Note

IRT "high flexibility" cannot be used for isochronous applications.

IRT "high performance"

In addition to the bandwidth reservation, the telegram traffic can be further tuned by configuring the topology. This enhances the performance during data exchange and the deterministic behavior. The IRT time interval can thus be further tuned or minimized with respect to IRT "high flexibility".

In addition to the isochronous data transfer provided by IRT, even the application itself (position control cycle, IPO cycle) can be isochronous in the devices. This is an essential requirement for closed-loop axis control and synchronization via the bus. Isochronous data transfer with cycle times well below one millisecond and with a deviation in the cycle start (jitter) of less than a microsecond provide sufficient performance reserves for demanding motion control applications.

In contrast to standard Ethernet and PROFINET IO with RT, the telegrams for PROFINET IO with IRT are transferred according to a schedule.

Modules

The following S110/S120 modules support the IRT "high performance":

- S120 CU320 together with the CBE20
- S120 CU320-2 DP together with the CBE20
- S120 CU320-2 PN
- S120 CU310 PN
- S120 CU310-2 PN
- S110 CU305 PN

Clock generation via PROFINET IO (isochronous communication)

SINAMICS S120 with CU310-2 PN/CU320-2 DP/CU320-2 PN can only assume the role of a synchronization device within a PROFINET IO network.

For a CU310-2 PN/CU320-2 DP/CU320-2 PN with CBE20 module, the following applies:

- Transmission type IRT, IO device is synchronization slave and isochronous, send cycle is applied to bus: Control Unit synchronizes with the bus and the send cycle becomes the cycle for the Control Unit.
- RT or IRT (option drive unit "not isochronous") has been configured. SINAMICS uses the local cycle configured in SINAMICS.

The following applies to a CU320-2 DP/CU320-2 PN for which a CBE20 is configured, but does not actually exist:

- SINAMICS uses the local clock (clock configured in SINAMICS); if there is no data exchange via PROFINET, alarm A01487 is output ("Topology: Comparison option slot components missing in the actual topology").
  Access via PROFINET is not available.

Comparison between RT and IRT

Table A-12 Comparison between RT and IRT

	RT	IRT "high flexibility"	IRT "high performance"
Transfer mode	Switching based on the MAC address; prioritization of the RT telegrams possible using Ethernet-Prio (VLAN tag).	Switching using the MAC address; bandwidth reservation by reserving an IRT "high flexibility" interval in which only IRT "high flexibility" frames are transferred but, for example, no TCP/IP frames.	Path-based switching according to a topology-based plan; no transmission of TCP/IP frames and IRT "high flexibility" frames in the IRT "high performance" interval.
Isochronous application in the IO controller	No	No	Yes
Determinism	Variance of the transmission duration by started TCP/IP telegrams.	Guaranteed transmission of the IRT "high flexibility" telegrams in the current cycle by the reserved bandwidth.	Exactly planned transfer; times for transmission and receiving are guaranteed for any topologies.
Reload the network configuration after a change	Not relevant	Only when the size of the IRT "high flexibility" interval needs to be modified (reservation of position is possible).	Always when the topology or the communications relationships change.
Maximum switching depth (number of switches in one line)	10 at 1 ms	61	64
For possible send cycles, see subitem "Send cycles and update cycles for RT classes" in table "Adjustable send cycles and update cycles"			

Set the RT class

The RT class is set by means of the properties of the controller interface of the IO controller. If RT class IRT "high performance" is set, it is not possible to operate any IRT "high flexibility" devices on the IO controller and vice versa. IO devices with RT can always be operated, regardless of the IRT class setting.

You can set the RT class in the HW Config for the associated PROFINET device.

1. In HW Config, double-click item PROFINET interface in the module.
   The "Properties" dialog box opens.
2. Select the RT class under RT class on the "Synchronization" tab.
3. Once you have selected "IRT", you can also choose between option "high flexibility" and "high performance".
4. Confirm with "OK".

Synchronization domain

The sum of all devices to be synchronized form a synchronization domain. The whole domain must be set to a single, specific RT class (real-time class) for synchronization. Different synchronization domains can communicate with one another via RT.

For IRT, all IO devices and IO controllers must be synchronized with a common synchronization master.

RT allows an IO controller to communicate with a drive unit outside a synchronization domain or "through" another synchronization domain. As of version 5.4 SP1, STEP 7 supports multiple synchronization domains on a single Ethernet subnet.

Example:

- Synchronization domain IRT: SIMOTION2 with SINAMICS
- SINAMICS drive that is assigned to the I/O system of SIMOTION1. This is arranged in the topology in such a way that its RT communication must be established through the IRT synchronization domain.

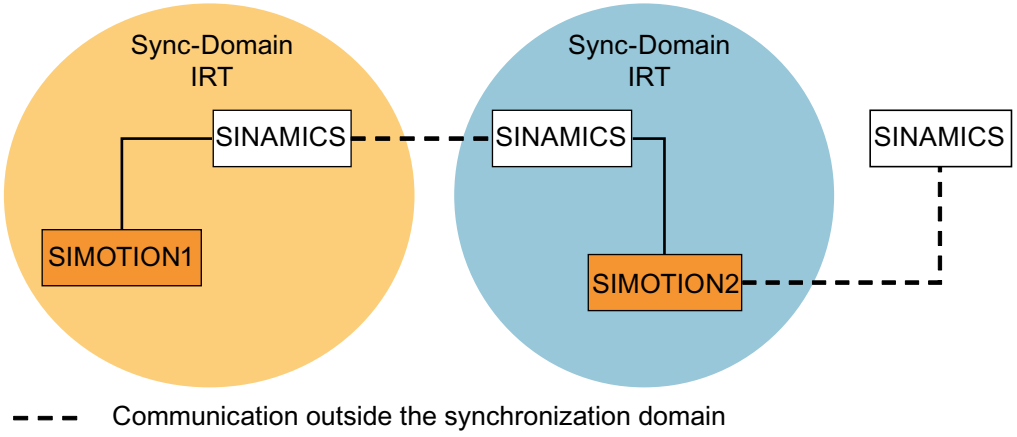


Figure A-30 RT communication across the limits of synchronization domains

Update cycles and send cycles for RT classes

Definition of the update time / send cycle:

If we take a single IO device in the PROFINET IO system as an example, this device has been supplied with new data (outputs) by the IO controller and has transferred new data (inputs) to the IO controller within the update time. The send cycle is the shortest possible update cycle.

All cyclic data is transferred within the send cycle. The actual send cycle that can be set depends on various factors:

- Bus load
- Type of devices used
- Computing capacity available in the IO controller
- Supported send clocks in the participating PROFINET devices of a synchronization domain. A typical send cycle is 1 ms.

The table below specifies the reduction ratios which can be set between the send cycle and the update times for IRT "high performance", IRT "high flexibility", and RT.

Table A-13 Settable send cycles and update cycles

Send cycle		**Reduction ratios between update time and send cycles**	
		RT **IRT "high flexibility"** [4]	**IRT "high performance"**
Range "even" [1]	250, 500, 1000 µs	1, 2, 4, 8, 16, 32, 64, 128, 256, 512	1, 2, 4, 8, 16[2]
	2000 µs	1, 2, 4, 8, 16, 32, 64, 128, 256	1, 2, 4, 8, 16[2]
	4000 µs	1, 2, 4, 8, 16, 32, 64, 128	1, 2, 4, 8, 16[2]
Range "odd" [3]	375, 625, 750, 875, 1125, 1250 µs ... 3875 µs (increment 125 µs)	Not supported[5]	1

Explanations for the above table:

1) It is only possible to set send cycles from the "even" range when IO devices with real-time class "RT" are assigned to a synchronization domain. Likewise, only the reduction ratios from the "even" range can be set for a send cycle setting from the "even" range.

2) It is generally only possible to set a reduction ratio of 1:1 between the update time and send cycle for IO devices (ET200S IM151-3 PN HS, SINAMICS S) which are operated in isochronous mode. In this case, the update cycle mode must always be set to "fixed factor" (under IO device properties, "IO cycle" tab, "Mode" pulldown menu). This means that STEP 7 will not automatically adjust the update cycle and thus the update cycle will always correspond to the send cycle.

3) The send cycles from the "odd" range can be set only if a synchronization domain does not include any IO devices with real-time class "RT". Likewise, only the reduction ratios from the "odd" range can be set for a send cycle setting from the "odd" range.

4) Isochronous operation is not compatible with IRT "high flexibility".

5) Odd send cycles can be used only if the IO systems assigned to the synchronization domain do not include any RT or IRT "high flexibility" devices.

Furthermore, the send cycles which can actually be set are determined by the intersection of the send cycles supported by all the devices in the synchronization domain.

The reduction ratio between the update cycle of an IO device and the send cycle is set in the "Properties" of the PROFINET interface for the relevant device.

Note

There is no intersection between the send cycles for the "even" and "odd" ranges!

Send cycles for SINAMICS drive units

A SINAMICS drive unit with PROFINET interface which supports IRT permits send cycle settings of between 0.25 ms and 4.0 ms in a 250 µs time frame.

Topology rules

Topology rules for RT

- A topology can be, but need not be configured for RT. If a topology has been configured, the devices must be wired in accordance with the topology.
- Otherwise, the wiring between devices is entirely optional.

Topology rules for IRT

- Mixed operation is not supported by STEP 7 V5.4 SP4, i.e. IRT "high performance" cannot be combined with IRT "high flexibility" in the same synchronization domain.
- A synchronization domain with IRT "high performance" can contain a maximum of one IRT "high performance" island. "Island" means that the devices must be interconnected to match the configured topology. A synchronization master must be positioned in the relevant island.
- IRT "high flexibility" is subject to the same topology rules as for IRT "high performance", the only exception being that a topology does not need to be configured. However, if a topology has been configured, the devices must be wired to match the topology.

Device selection in HW Config

Hardware catalog

The drive unit from the appropriate device family entry in the hardware catalog must be configured. For the real-time class IRT, these are all entries as of firmware version V2.5.

GSDML

GSDML files for devices which contain IRT as of firmware version V2.5.

A.1.3.3 PROFINET GSDML

SINAMICS S120 supports the GSDML version: "PROFINET GSDML" to embed the converter in a PROFINET network.

PROFINET GSDML allows standard telegrams to be combined with a PROFIsafe telegram – and if required, a telegram extension. Each of the modules has four subslots: The Module Access Point (MAP), the PROFIsafe telegram, a PZD telegram to transfer process data and where necessary, a telegram for PZD extensions. Example:

GSDML-V2.31-Siemens-Sinamics_S_CU3x0_20160101.xml

You can download GSDML files from the following Siemens Internet address:

PROFINET GSDML (https://support.industry.siemens.com/cs/ww/en/view/49217480)

The GSDML files on the memory card are saved in the following location: ..\SIEMENS\SINAMICS\DATA\CFG\PNGSD.ZIP

Submodules depending on the particular drive object

The following table shows the possible submodules depending on the particular drive object.

Table A-14 Submodules depending on the particular drive object

Module	Sub-slot 1 MAP	Subslot 2 PROFIsafe	Subslot 3 PZD telegram	Subslot 4 PZD extension	Subslot 5	Max. num-ber of PZD
SERVO	MAP	Telegram 30/31/901/902/903	Telegrams: 1...220 free PZD-16/16	Supplementary telegrams 700/701/750, PZD-2/2, -2/4, -2/6, -8/8	Supplementary telegrams 700/701/750, PZD-2/2, -2/4, -2/6, -8/8	20/28
VECTOR	MAP	Telegram 30/31/901/902/903	Telegrams: 1...352 free PZD-16/16, 32/32	Supplementary telegrams 700/701/750, PZD-2/2, -2/4, -2/6, -8/8	Supplementary telegrams 700/701/750, PZD-2/2, -2/4, -2/6, -8/8	32/32
Infeed	MAP	Reserved	Telegrams: 370, 371 free PZD-4/4	PZD-2/2, -2/4, -2/6	Reserved	10/10
Encoder	MAP	Reserved	Telegrams: 81, 82, 83 free PZD-4/4	PZD-2/2, -2/4, -2/6	Reserved	4/12
TB30, TM31, TM15 DI_DO, TM120	MAP	Reserved	Telegrams: no free PZD-4/4	Reserved	Reserved	5/5
TM150	MAP	Reserved	Telegrams: no free PZD-4/4	Reserved	Reserved	7/7
TM41	MAP	Reserved	Telegrams: 3 free PZD-4/4, 16/16	Reserved	Reserved	20/28
Control Unit	MAP	Reserved	Telegrams: 390, 391, 392, 393, 394, 395 free PZD-4/4	Reserved	Reserved	5/21
TM15/TM17	Not supported.					

The telegrams in subslots 2, 3 and 4 can be freely configured, i.e. they can also remain empty.

Configuration

1. Insert a "DO SERVO/VECTOR/..." module.
2. Insert the optional submodule "PROFIsafe telegram 30".
3. Insert a submodule "PZD telegram xyz".
4. Insert the optional submodule "PZD extension".
5. Assign the I/O addresses for the module and the submodules.

You will find a detailed description for processing a GSDML file in HW Config in the SIMATIC documentation.

A.1.3.4 Motion Control with PROFINET

Motion Control / isochronous drive link with PROFINET

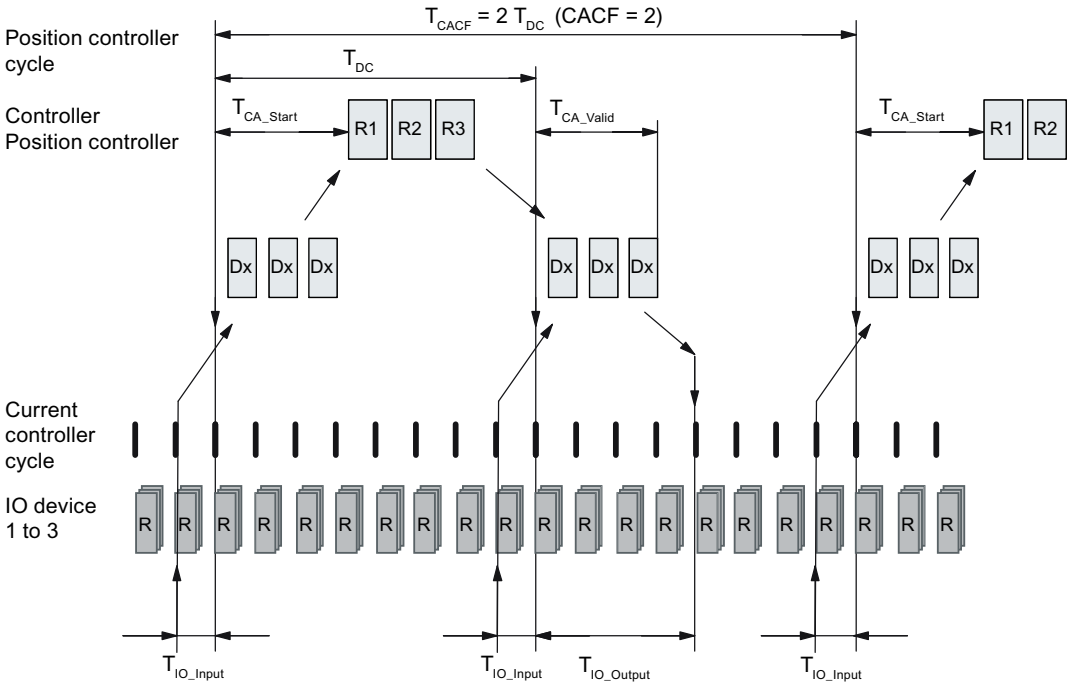


Figure A-31 Motion Control / isochronous drive link with PROFINET, optimized cycle with CACF = 2 (Controller Application Cycle Factor)

When planning the communication system, please observe the following interrelationships between the synchronism of the communication and your specific application:

- Isochronous data transfer
  With the PROFINET IRT (Isochronous Real Time) communication profile, PROFINET provides a mechanism for isochronous data transfer. Details are provided in Chapter "RT classes for PROFINET IO (Page 150)".
- Synchronous applications
  - An isochronous application involves an application where it is necessary to have a precise correlation of the process data with respect to time (process data image that is consistent over time). Process data are transferred with a synchronized communication.
  - You must synchronize the application to the communication cycle so that the bus and the application can interact with one another. This means that you can directly correlate all process data of a communication cycle with respect to time.

Sequence of data transfer to closed-loop control system

1. Actual position value G1_XIST1 is read into the telegram image at time T_{IO_Input} before the start of each clock cycle - and transferred to the controllers in the next cycle.
2. Closed-loop control of the controller starts at time T_{CA_Start} after each position controller cycle and uses the current actual values read previously from the devices.
3. In the next cycle, the controller transfers the calculated setpoints to the telegram image of the device. The speed setpoint command NSET_B is issued to the closed-loop control system at time T_{IO_Output} after the beginning of the cycle.

Note

With the isochronous telegram setting, the complete SINAMICS device is in clock cycle synchronism with all data. Reasons:

- Between the controller and device, all data are only exchanged in one IRT frame.
- In SINAMICS, all data are consistently processed in synchronism.

Designations and descriptions for motion control

Table A-15 Time settings and meanings

Name	Limit value	Description
T_{DC_BASE}	-	Time basis for cycle time T_{DC} calculation: T_{DC_BASE} = T_DC_BASE · 31.25 µs = 4 · 31.25 µs = 125 µs
T_{DC}	T_DC_MIN ≤ T_DC ≤ T_DC_MAX	Cycle time T_{DC} = T_DC · T_{DC_BASE} ,T_DC: integer factor CBE20: T_{DC_MIN} = T_DC_MIN · T_{DC_BASE} = 4 · 125 µs = 500 µs T_{DC_MAX} = T_DC_MAX · T_{DC_BASE} = 32 · 125 µs = 4 ms X150 (CU3x0-2 PN): T_{DC_MIN} = T_DC_MIN · T_{DC_BASE} = 2 · 125 µs = 250 µs T_{DC_MAX} = T_DC_MAX · T_{DC_BASE} = 32 · 125 µs = 4 ms
T_{CACF}	CACF = 1-14	IO controller application cycle time This is the time frame in which the IO controller application generates new setpoints (e.g. in the position controller cycle). Calculation example: T_{CACF} = CACF · T_DC = 2 · 500 µs = 1 ms
T_{CA_Valid}	$T_{CA\_Valid} < T_{DC}$	Time, measured from the beginning of the cycle, at which the actual values of all IO devices for the controller application process (position control) are available.
T_{CA_Start}	$T_{CA\_Start} > T_{CA\_Valid}$	Time, measured from the beginning of the cycle, at which the controller application process (position control) starts.
T_{IO_BASE}		Timebase for T_{IO_Input}, T_{IO_Output} T_{IO_BASE} = T_IO_BASE · 1 ns = 125000 · 1 ns = 125 µs

Name	Limit value	Description
T_{IO_Input}	T_IO_InputMIN ≤ T_IO_Input < T_DC	Time of actual value acquisition This is the time at which actual values are acquired before a new cycle starts. T_{IO_Input} = T_IO_Input · T_{IO_BASE} T_IO_Input: integer factor
	$T_{IO\_InputMIN}$	Minimum value for T_{IO_Input} Calculation: $T_{IO\_InputMIN}$ = T_IO_InputMIN · T_{IO_BASE} = 375 µs
T_{IO_Output}	T_IO_Output_valid + T_IO_OutputMIN ≤ T_IO_Output < T_DC	Time of setpoint transfer This is the time, calculated from the beginning of the cycle, at which the transferred setpoints (speed setpoint) are accepted by the closed-loop control system. T_{IO_Output} = T_IO_Output · T_{IO_BASE} T_IO_Output: integer factor
	$T_{IO\_OutputMIN}$	Minimum value for T_{IO_Output} Calculation: $T_{IO\_OutputMIN}$ = T_IO_OutputMIN · T_{IO_BASE} = 250 µs
	T_IO_Output_valid	The time after which the new control output data (setpoints) is available for the drive object.
Dx		Data_Exchange This service is used to implement user data exchange between the IO controller and IO device 1 - n.
R or Rx		Computation time, current or position controller

Setting criteria for times

- Cycle (T_{DC})
  - T_{DC} must be set to the same value for all bus nodes. T_{DC} is a multiple of SendClock.
  - $T_{DC} > T_{CA\_Valid}$ and $T_{DC} \geqq T_{IO\_Output}$
    T_{DC} is thus large enough to enable communication with all bus nodes.
- T_{IO_Input} and T_{IO_Output}
  - Setting the times in T_{IO_Input} and T_{IO_Output} to be as short as possible reduces the dead time in the position control loop.
  - $T_{IO\_Output} > T_{CA\_Valid} + T_{IO\_Output\_MIN}$
- Settings and tuning can be done via a tool (e.g. HW Config in SIMATIC S7).

User data integrity

User data integrity is verified in both transfer directions (IO controller <––> IO device) by a sign-of-life (4-bit counter).

The sign-of-life counters are incremented from 1 to 15 and then start again at 1.

- IO controller sign-of-life
  - STW2.12 ... STW2.15 are used as the IO controller sign-of-life.
  - The IO controller sign-of-life counter is incremented in each IO controller application cycle (T_{CACF}).
  - The number of sign-of-life errors tolerated can be set via p0925.
  - p0925 = 65535 deactivates sign-of-life monitoring on the IO device.
  - Monitoring
    The IO controller sign-of-life is monitored on the IO device and any sign-of-life errors are evaluated accordingly.
    The maximum number of tolerated IO controller sign-of-life errors in succession can be set via p0925.
    If the number of tolerated sign-of-life errors set in p0925 is exceeded, the response is as follows:
    1. A fault (F01912) is output.
    2. The value "0" is output as the IO device sign-of-life.
    3. A new synchronization (at least 15 received correct signs-of-life in succession) with the IO controller sign-of-life is started.
    One sign-of-life error can be reset with ten correct signs-of-life in succession.
- IO device sign-of-life
  - ZSW2.12 ... ZSW2.15 are used as the IO device sign-of-life.
  - The IO device sign-of-life counter is incremented in each DC cycle (T_{DC}).
  - Monitoring of the IO device sign-of-life can be implemented in the controller application.

Overview of important parameters (see SINAMICS S120/S150 List Manual)

T_{DC}	r2064[1]	PB/PN diagnostics isochronous operation: Bus cycle time
T_{CACF}	r2064[2]	PB/PN diagnostics isochronous operation: Master cycle time
T_I	r2064[3]	PB/PN diagnostics isochronous operation: Instant that the actual value is acquired
T_O	r2064[4]	PB/PN diagnostics isochronous operation: Instant that the setpoint is acquired

A.1.3.5 Communication with CBE20

The CBE20 is a flexibly usable communications module that can operate with different communication profiles. You can only load the firmware of a communication profile at any one time. The available firmware files are saved with the communication profiles in UFW files on the Control Unit memory card. Firmware can only be selected prior to commissioning.

Select the required file via parameter p8835. Carry out a POWER ON after selecting the required UFW file. During the subsequent system boot, the corresponding UFW file is loaded. The new selection then becomes active.

Table A-16 Functionality and selection in the pointer file

Functionality (p8835)	Content	Detailed information on this is provided in Chapter:
PROFINET device	1	-
PROFINET Gate	2	"Communication via PROFINET Gate (Page 161)"
SINAMICS Link	3	"Communication via SINAMICS Link (Page 221)"
EtherNet/IP	4	"Communication via Ethernet/IP (EIP) (Page 203)"
Modbus TCP	5	"Communication via Modbus TCP (Page 188)"
Customer-specific[1)] from OEM directory	99	-

1) Path for the UFW file and folders on the memory card: /OEM/SINAMICS/CODE/CB/CBE20.UFW

Identification of the firmware version

Parameter r8858 can uniquely identify the loaded firmware version of the PROFINET interface.

Overview of important parameters (see SINAMICS S120/S150 List Manual)

- p8835 CBE20 firmware selection
- r8858[0...39] COMM BOARD read diagnostics channel
- r8859[0...7] COMM BOARD identification data

A.1.3.6 Communication via PROFINET Gate

The "PN GATE FOR SINAMICS" is a PROFINET solution for controller manufacturers or mechanical equipment manufacturers who wish to simply integrate an interface to a PROFINET network in their controllers. PROFINET communication is implemented via the standard Ethernet interface of the controller without the need for a communication module or an option module.

"PN GATE FOR SINAMICS" enables control devices with a standard Ethernet interface to be connected isochronously via PROFINET with IRT to SINAMICS S120 and motion control, robotics or CNC applications to be implemented with SINAMICS S120 drives. In addition to the SINAMICS S120, other PROFINET devices (drives, distributed I/O, etc.) can be connected.

Possible drive units:

- CU320-2 PN

The CBE20 in the CU320-2 PN of the SINAMICS S120 contains the "PN Gate" function (p8835 = 2). The PN Gate represents the controller in the sense of PROFINET. It covers a standard PROFINET network.

The CBE20 (port 4) is connected via the standard Ethernet interface of the machine control.

The controller supplies the PROFINET controller in the CBE20 with the content required for all the I/O data cyclically and in a compact form in one or more Ethernet telegrams. For this purpose, a driver (part of the PN Gate) is used on the controller for the communication with the CBE20.

The CBE20 then distributes the I/O data to each individual device in the PROFINET network with one telegram in each case - both IRT and RT telegrams.

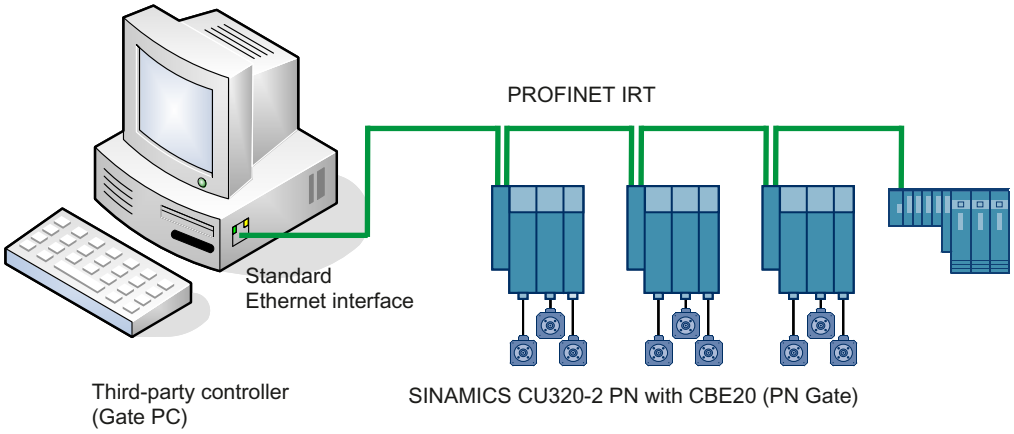


Figure A-32 Schematic representation of SINAMICS PROFINET Gate (in short: PN Gate)

Functions supported by PN Gate

PN Gate function overview

Function	Description
Communication channels	• Cyclic data communication: – IRT – RT • Acyclic data communication: – PROFINET alarms – Read/write data record – TCP/IP
PROFINET basic services	• LLDP • DCP • SNMP
Accesses to process data	Access to the process image: • Subslot granular • Device granular
Consistency of the cyclic data	Each process data communication cycle can contain a data component for IRT and RT communication

Function	Description
Network topologies	• Line • Star • Tree
Information from the PN Gate	• Device number • Slot number with the associated subslot numbers • IO address • Diagnostic addresses • Module ID (vendor ID and module ID) • Send cycles and update times
Activating/deactivating	Activating and deactivating devices via the API without alarm triggering
Automatic address assignment	Topology-based initialization
Number of IO devices	A maximum of 64 devices
IO area in the controller	• 4096 bytes each, in and out • Maximum number of slots: 2048 • Maximum bytes per slot/module size: 254 bytes
Send cycle	• RT communication: 1 ms Update times RT 2^n with n = 0 to 9x send cycle • IRT communication 1 ms ... 4 ms in increments of 250 µs minimum send cycle of 1 ms for 32 devices. It is permissible to reduce the data per device.

Preconditions for PN Gate

Hardware

- SINAMICS CU320-2 PN with firmware version as of 4.5
- Communication Board Ethernet 20 (CBE20)
- Short Ethernet cable to connect CBE20 and CU320-2 PN (X150)
  Recommendation: Ethernet cable with the article number: 6SL3060-4AB00-0AA0
- Control hardware with standard Ethernet interface (100 Mbit/s or higher),
  for example, the SIMATIC Box IPC 427C.

Note

The Gate PC must guarantee the short latency times required for operating the PN Gate. Influencing variables are the CPU performance, mainboard hardware (Ethernet chipset and its connection), and the BIOS and the software components involved (operating system components such as memory mapping, Ethernet driver, interrupt link, configuration).

Software

- STARTER as of V4.3

  Note
  Startdrive

  Please note that you still cannot use this function with Startdrive.

  or

- Drive ES as of V5.5
  or
- SIMATIC STEP 7 as of V5.5 SP2
- Development kit for the development and configuration:
  - SINAMICS PN Gate DevKit (Article No. 6SL3071-0CA00-0XA0)
- Licenses
  - The PN Gate CU requires a runtime license with Article No. 6SL3074-0AA03-0AA0 or the Z option G01 for CFC.

PROFINET version

- SINAMICS PN Gate V2 is compatible with PROFINET V2.2

Scope of delivery PN Gate Dev Kit (Development Kit)

The PN Gate development kit is supplied on a DVD and contains the following components:

- STEP 7 add-on setup
  - CD1
    PN Gate add-on setup for STEP7 5.5 SP2, STARTER 4.3, SINAMICS 4.5
- PN Gate driver
  - Bin
    Binary files of the driver in the Tar format.
  - Src
    Source files as a zip file and unzipped.
  - Doc
    Doxygen documentation as zip file. The Doxygen documentation is available in HTML and PDF format.
- Application example
  - PROFIdrive sample applications in binary and in source code.
- Documentation
  - German
    PN Gate documentation in German.
  - English
    PN Gate documentation in English.

You can find additional information in the "SINAMICS 120 PN Gate Configuration Manual".

A.1.3.7 PROFINET with 2 controllers

Control Unit settings

Note

Operation with two controllers is only possible in conjunction with an F-CPU.

SINAMICS S120 allows 2 controllers to be connected simultaneously to a Control Unit via PROFINET, e.g. an automation controller (A-CPU) and a safety controller (F-CPU).

SINAMICS S supports for this communication the PROFIsafe standard telegrams 30 and 31, as well as the Siemens telegrams 901, 902 and 903 for the safety controller.

Example

The following diagram shows a configuration example of a drive with three axes. The A-CPU sends Siemens telegram 105 for axis 1 and Siemens telegram 102 for axis 2. The F-CPU sends PROFIsafe telegram 30 for axis 1 and axis 3.

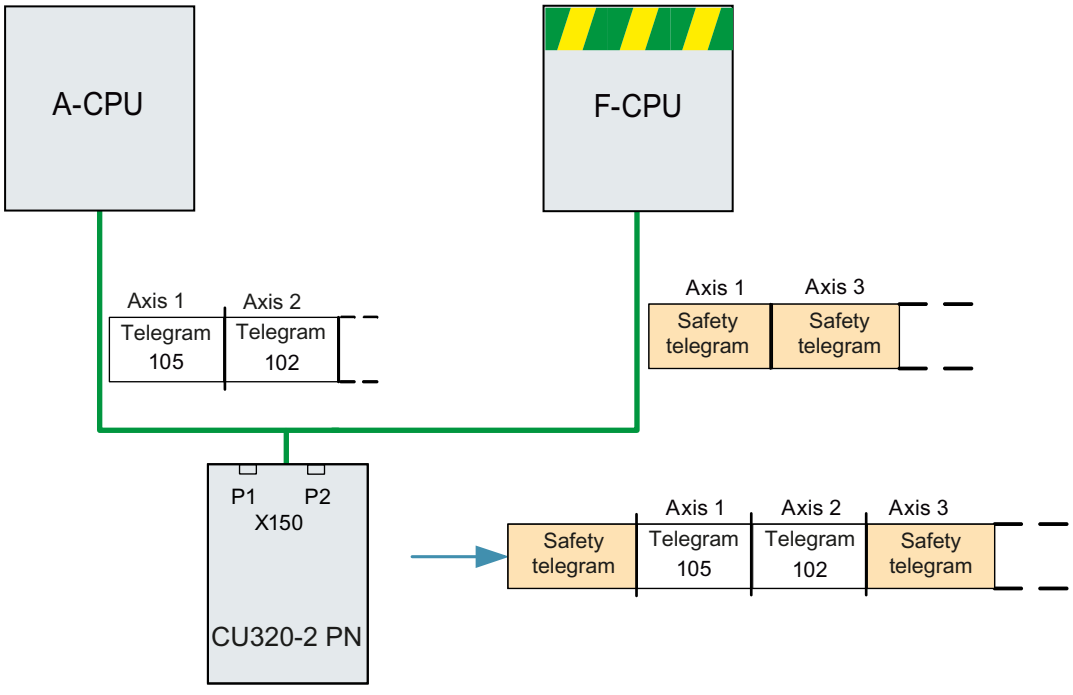


Figure A-33 Example, communication sequence

Configuration

To configure the connection, proceed as follows:

1. Using parameters p9601.3 = p9801.3 = 1, enable PROFIsafe for axes 1 and 2.
2. Configure the PROFINET communication in HW Config (see section "Configuring the controllers").
   The controller establishes the communication.

Note

When booting, the drive system first requires the configuration data of A-CPU and then establishes a cyclic communication to this CPU taking into account the PROFIsafe telegrams expected.

As soon as the drive system has received the configuration data of the F-CPU, then cyclic communication is also established here and PROFIsafe telegrams are taken into consideration.

Note

CPU failure

Communication is carried out by both controllers independently of one another. In the event of failure of a CPU, communication with the other CPU is not interrupted, it continues to operate without interruption. Error messages are output regarding the components that have failed.

- Resolve the fault and acknowledge the messages. Communication to the CPU that failed is then automatically restored.

Configuring the shared device

Note

Startdrive

Please note that you still cannot use this function with Startdrive.

You have the following 2 options in "HW Config" when configuring the two controllers A-CPU and F-CPU:

- You configure both of the controllers using the shared device function in a common project
- Using GDSML, you configure each controller independently in its own project

The first of these options is described in the following example.

Note

Detailed information on configuring with "HW Config " is provided in the STEP 7 documentation.

Example: 2 controllers in a common project

Proceed as follows in the specified sequence:

- Required steps in STEP 7 (Page 167)
- Required steps in STARTER (Page 169)
- Configuring the Safety control (Page 171)
- Inserting the PROFIsafe controller in STEP 7 (Page 172)
- Configuring the F-CPU in HW Config (Page 173)

Required steps in STEP 7

Start STEP 7

1. Under S7, create an automation controller for the new project, in the example called A-CPU, based on a SIMATIC 300.

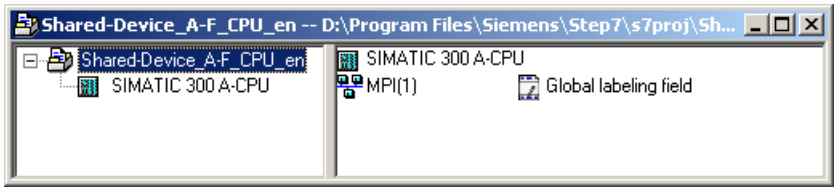


Figure A-34 Creating a new S7 project

2. In HW Config, select the controller CPU 315-2 PN/DP and connect the PROFINET IO as a communication network.
3. Select an S120 drive from the object manager (in the example, a CU320-2 PN).

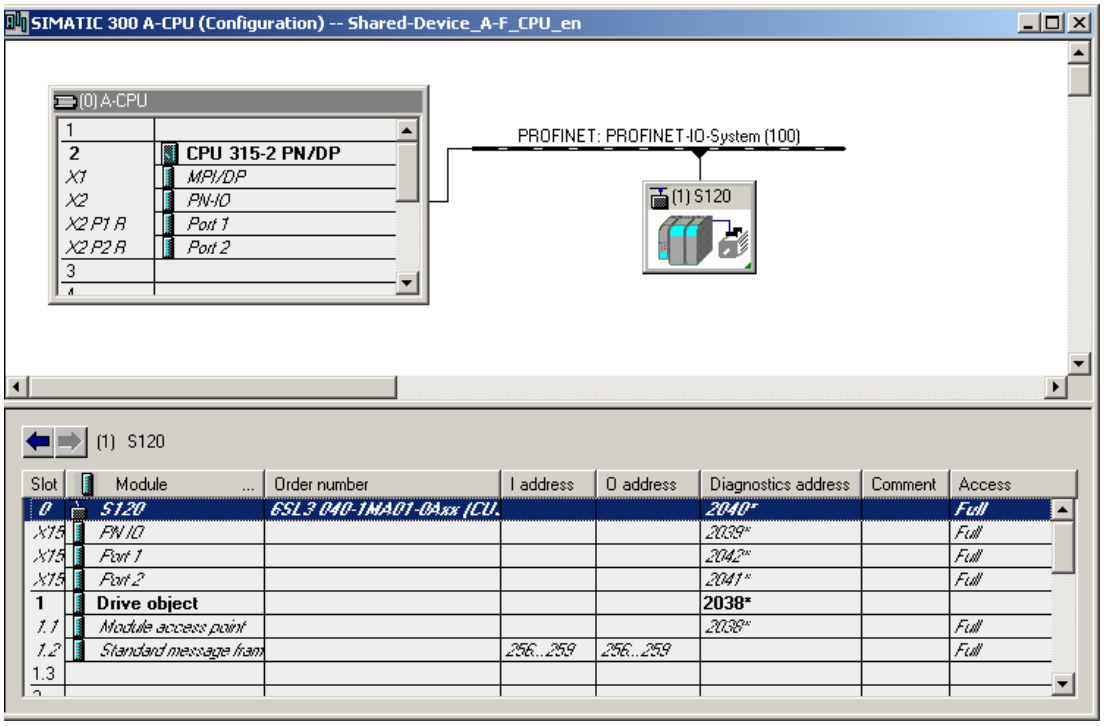


Figure A-35 Automation controller created in HW Config

4. Select menu "Station/save and compile" (Ctrl+S).
   The previous project is saved.
5. To configure the drives in STARTER, from the shortcut menu of the S120 drive, select "Open object with STARTER".

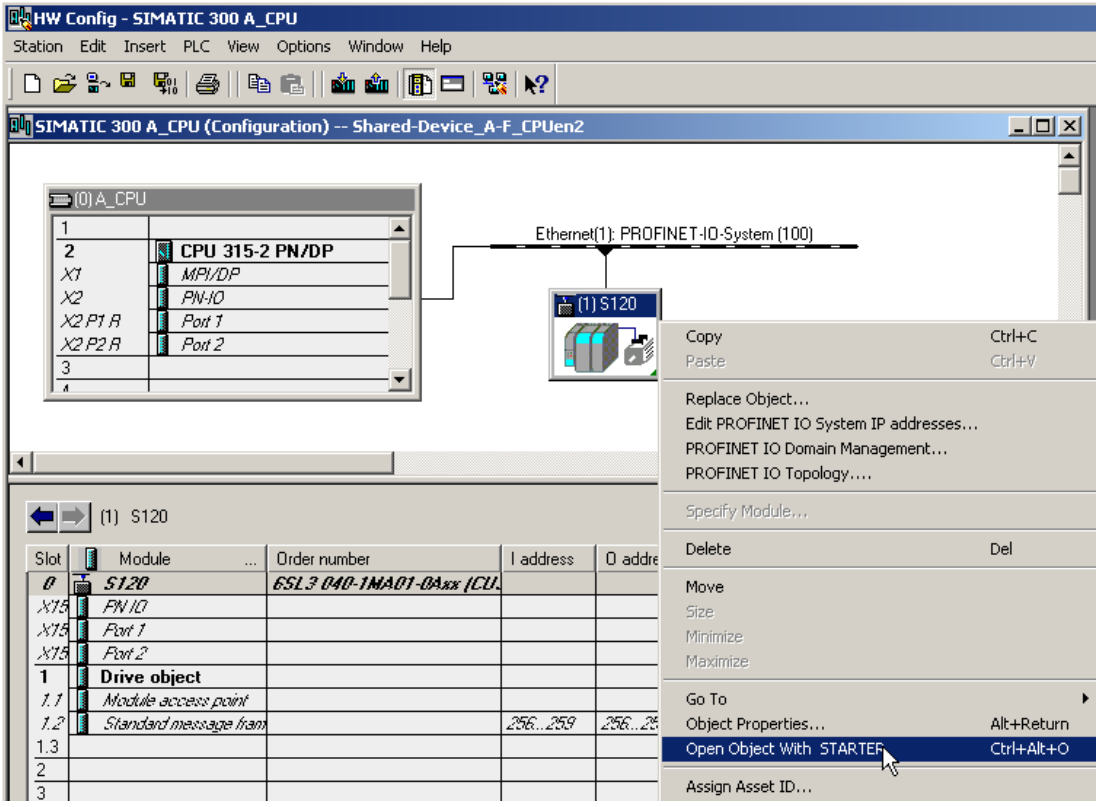


Figure A-36 New project transferred from HW Config into STARTER

Required steps in STARTER

Configuring telegrams in STARTER

The STARTER window opens automatically and shows the project in the navigation window.

1. Configure an infeed and three drives in servo control. We have selected telegram 370 for the infeed communication, and standard telegrams 1, 2 and 3 for the drives.
   - Then click under project "Save and recompile all".
   - Click in the navigation window "Communication \ Telegram Configuration".

Object	Drive object	-No.	Assigned controller	Message frame type		Input data		Output data	
						Length	Address	Length	Address
1	Supply_1	2		SIEMENS telegram 370, PZD-1/1	!	1	???..???	1	???..???
2	Drive_1	3		Standard telegram 1, PZD-2/2	!	2	???..???	2	???..???
3	Drive_2	4		Standard telegram 2, PZD-4/4	!	4	???..???	4	???..???
4	Drive_3	5		Standard telegram 3, PZD-5/9	!	9	???..???	5	???..???
5	Control_Unit	1	PN-IO	Free telegram configuration with BICO	!	2	256..259	2	256..259
Without PZDs (no cyclic data exchange)									

Figure A-37 Telegram overview for PROFIdrive channel IF1

2. Under ".....", add the safety telegrams 30 for the 1st and 3rd drive:
   - In the table, click the drive that you want to monitor with PROFIsafe.
   - Click the "Adapt telegram configuration" button and select "Add PROFIsafe".

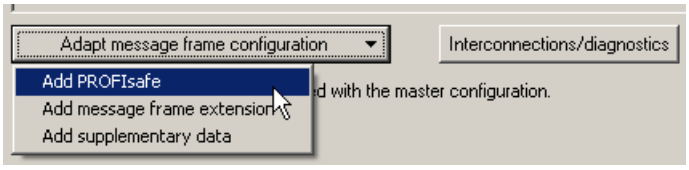


Figure A-38 Add the PROFIsafe telegram to the drive

The PROFIsafe telegrams were added to the PROFIdrive table:

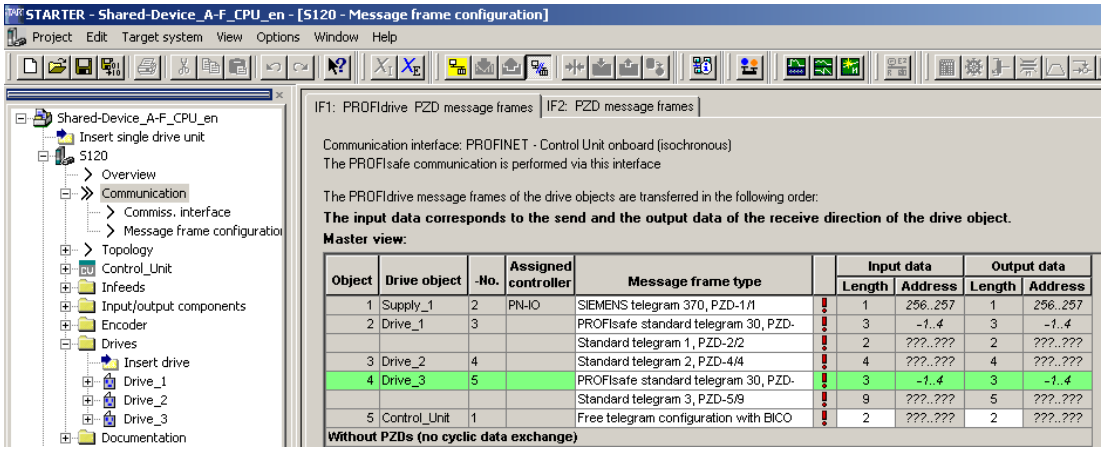


Figure A-39 List of telegrams that are available

3. To transfer your telegram changes into HW Config, click on "Set up addresses".

IF1: PROFIdrive PZD message frames | IF2: PZD message frames

Communication interface: PROFINET - Control Unit onboard (isochronous)
The PROFIsafe communication is performed via this interface

The PROFIdrive message frames of the drive objects are transferred in the following order:
The input data corresponds to the send and the output data of the receive direction of the drive object.
Master view:

Object	Drive object	-No.	Assigned controller	Message frame type		Input data		Output data	
						Length	Address	Length	Address
1	Control_Unit	1	PN-IO	Free telegram configuration with BICO	✔	2	256..259	2	256..259
2	Supply_1	2	PN-IO	SIEMENS telegram 370, PZD-1/1	✔	1	260..261	1	260..261
3	Drive_1	3	PN-IO-1	PROFIsafe standard telegram 30, PZD-	✔	3	0..5	3	0..5
			PN-IO	Standard telegram 1, PZD-2/2	✔	2	262..265	2	262..265
4	Drive_2	4	PN-IO	Standard telegram 2, PZD-4/4	✔	4	266..273	4	266..273
5	Drive_3	5	PN-IO-1	PROFIsafe standard telegram 30, PZD-	✔	3	6..11	3	6..11
			PN-IO	Standard telegram 3, PZD-5/9	✔	9	274..291	5	274..283
Without PZDs (no cyclic data exchange)									

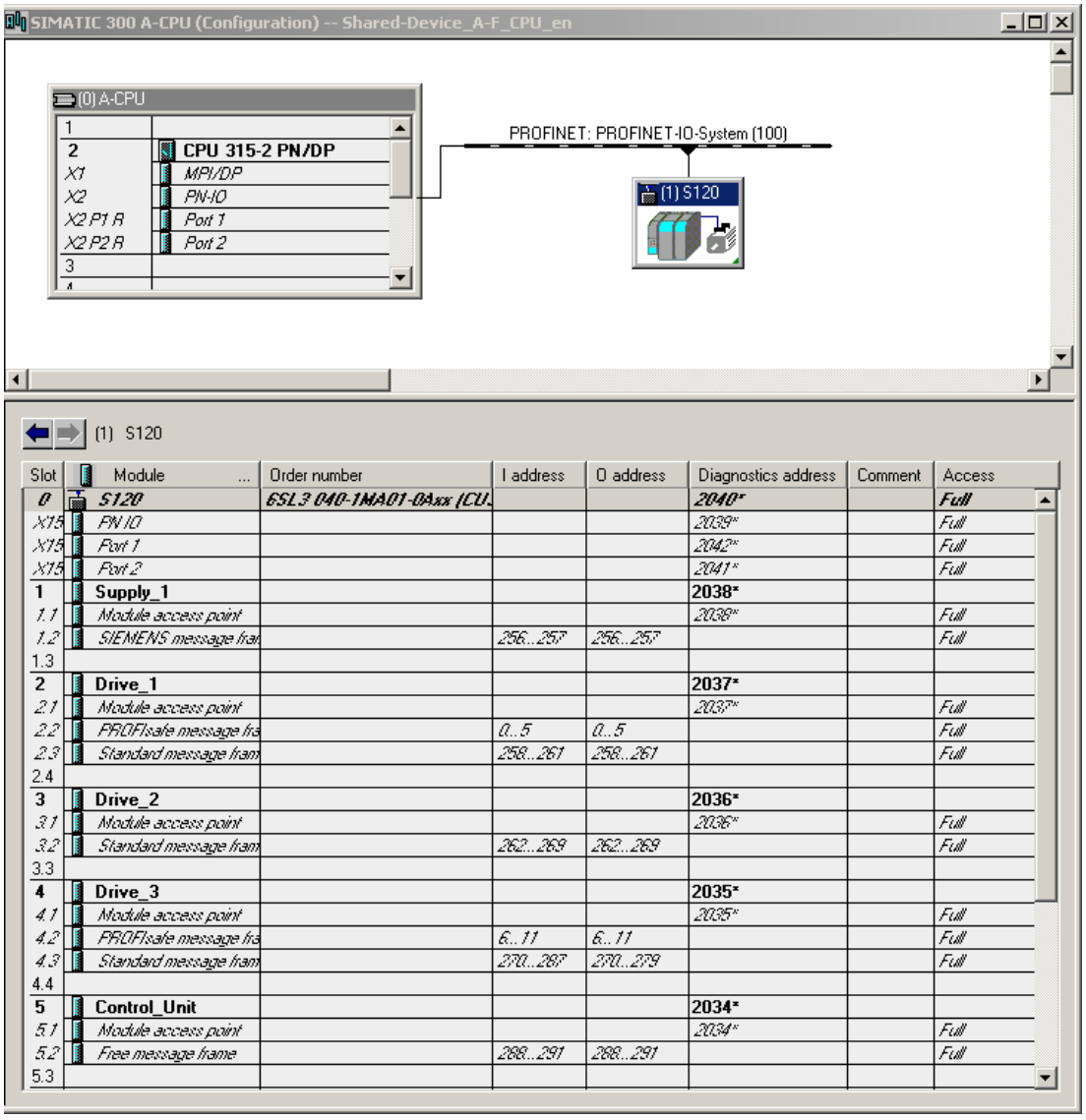
Figure A-40 The telegrams were aligned with HW Config

After the telegrams have been successfully transferred to HW Config, the red exclamation mark is replaced by a checkmark.

Configuring the Safety control

Enable telegrams

1. In the HW Config window, click the S120 drive.



Slot	Module	Order number	I address	O address	Diagnostics address	Comment	Access
0	S120	6SL3 040-1MA01-0Axx (CU			2040*		Full
X15	PN IO				2039*		Full
X15	Port 1				2042*		Full
X15	Port 2				2041*		Full
1	Supply_1				2038*		
1.1	Module access point				2038*		Full
1.2	SIEMENS message fra		256...257	256...257			Full
1.3							
2	Drive_1				2037*		
2.1	Module access point				2037*		Full
2.2	PROFIsafe message fra		0...5	0...5			Full
2.3	Standard message fram		258...261	258...261			Full
2.4							
3	Drive_2				2036*		
3.1	Module access point				2036*		Full
3.2	Standard message fram		262...269	262...269			Full
3.3							
4	Drive_3				2035*		
4.1	Module access point				2035*		Full
4.2	PROFIsafe message fra		6...11	6...11			Full
4.3	Standard message fram		270...287	270...279			Full
4.4							
5	Control_Unit				2034*		
5.1	Module access point				2034*		Full
5.2	Free message frame		288...291	288...291			Full
5.3							

Figure A-41 Updated project in HW Config

   There is full access to all telegrams. You must enable this in order that the PROFIsafe controller can access telegram 30.

2. From the shortcut menu of the S120 drive, select menu "Object properties...".
3. In the following window, you lock the access of the PROFIsafe telegrams through the A-CPU.

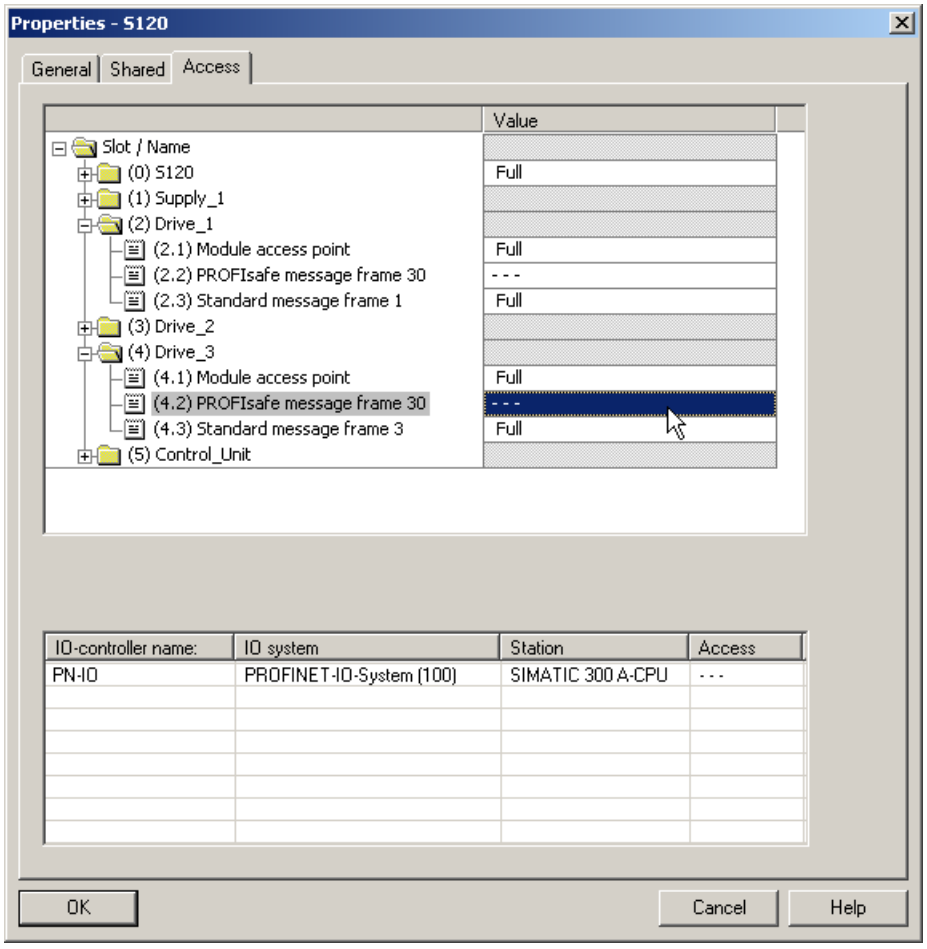


Figure A-42 Safety telegrams of the A-CPU enabled

Inserting the PROFIsafe controller in STEP 7

You configure the PROFIsafe controller in precisely the same way as the automation controller under STEP 7.

Configuring the F-CPU in HW Config

1. Contrary to an automation controller, you now select a PROFIsafe-compatible controller, for example, a CPU 317F-2 PN/DP.
   We have manually renamed the PROFIsafe controller to "F-CPU".
2. To establish the communication, select PROFINET IO again.

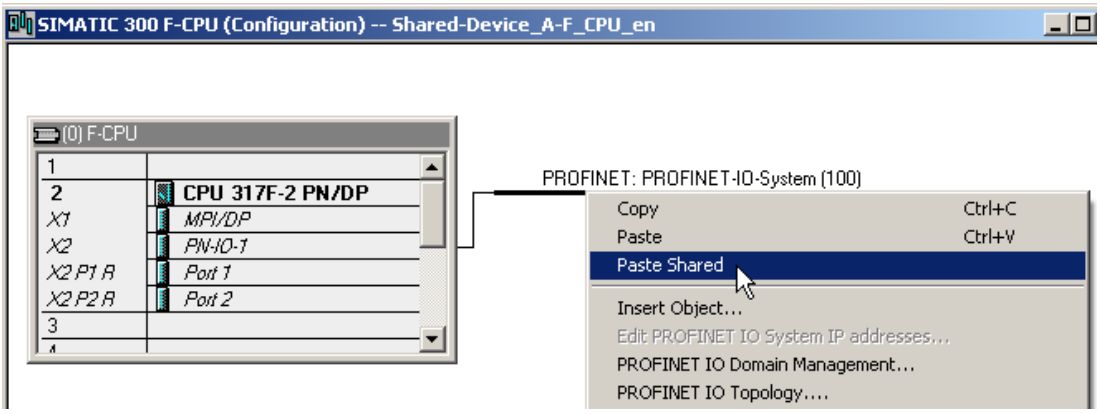


Figure A-43 PROFIsafe controller configuration

3. In HW Config, click "Station\Save and compile".
4. In the automation controller window, click the S120 drive.
5. In the menu, select "Edit/copy" to start copying.
6. Return to the HW Config window of the PROFIsafe controller.
7. Right-click the PROFINET line.

8. Select "Insert shared" in the shortcut menu.
   The S120 automation controller is connected to the PROFINET of the PROFIsafe controller. In the table, the PROFIsafe controller has automatically been allocated full access for PROFIsafe telegram 30.

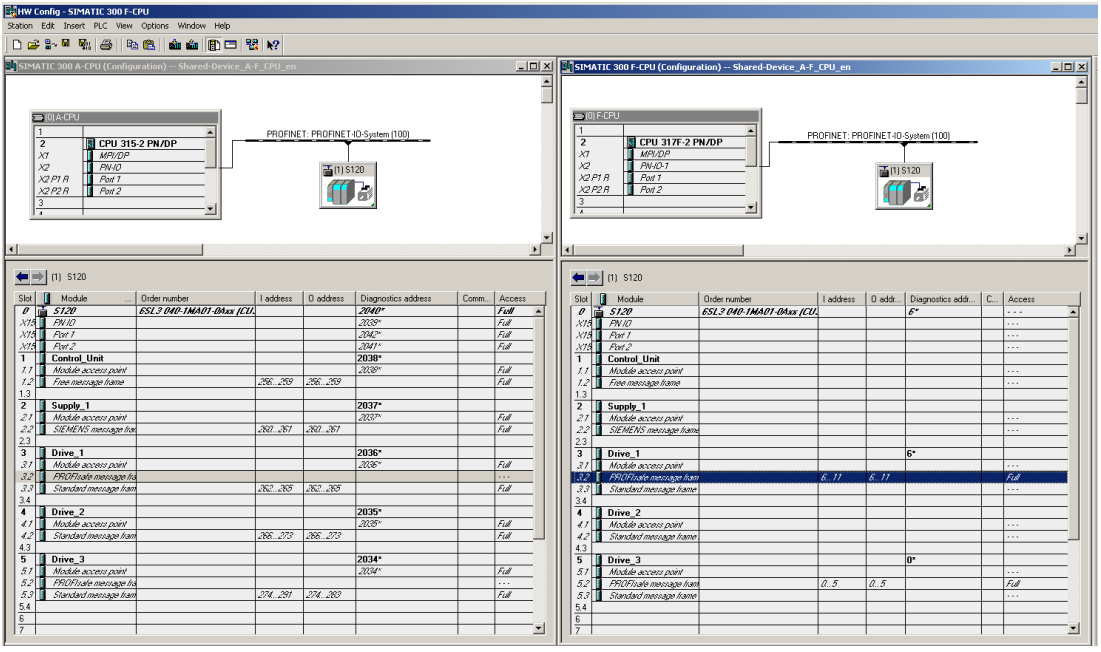


Figure A-44 New project completed in HW Config

9. In HW Config, click "Station\Save and compile".

10. Click "Open object with STARTER" again
    After completing the last save operation, you will see in the STARTER window that the PROFIsafe telegrams have been assigned to PN-IO-1 and the drive telegrams to PN-IO.

IF1: PROFIdrive PZD message frames | IF2: PZD message frames

Communication interface: PROFINET - Control Unit onboard (isochronous)
The PROFIsafe communication is performed via this interface

The PROFIdrive message frames of the drive objects are transferred in the following order:
The input data corresponds to the send and the output data of the receive direction of the drive object.
Master view:

Object	Drive object	-No.	Assigned controller	Message frame type		Input data		Output data	
						Length	Address	Length	Address
1	Control_Unit	1	PN-IO	Free telegram configuration with BICO	✔	2	256..259	2	256..259
2	Supply_1	2	PN-IO	SIEMENS telegram 370, PZD-1/1	✔	1	260..261	1	260..261
3	Drive_1	3	PN-IO-1	PROFIsafe standard telegram 30, PZD-	✔	3	0..5	3	0..5
			PN-IO	Standard telegram 1, PZD-2/2	✔	2	262..265	2	262..265
4	Drive_2	4	PN-IO	Standard telegram 2, PZD-4/4	✔	4	266..273	4	266..273
5	Drive_3	5	PN-IO-1	PROFIsafe standard telegram 30, PZD-	✔	3	6..11	3	6..11
			PN-IO	Standard telegram 3, PZD-5/9	✔	9	274..291	5	274..283
Without PZDs (no cyclic data exchange)									

Figure A-45 New project completed in STARTER

If there is a checkmark after each telegram type in STARTER, then the Shared Device has been successfully configured.

Overview of important parameters

Overview of important parameters (see SINAMICS S120/S150 List Manual)

- p9601 SI enable functions integrated in the drive (Control Unit)
- p9801 SI enable functions integrated in the drive (Motor Module)

A.1.3.8 PROFINET media redundancy

To increase the availability of PROFINET, you can create a ring topology. If the ring is interrupted at one point, the data paths between the devices are automatically reconfigured. Following reconfiguration, the devices can once again be accessed in the resulting new topology.

To create a ring topology with media redundancy, route the two ends of a line-type PROFINET topology to a switch which serves as redundancy manager (e.g. a suitable SCALANCE switch). Closing the linear bus topology is realized using two ports (ring ports) of the SCALANCE redundancy manager, which monitors the data telegrams in the PROFINET ring. All other connected PROFINET nodes are redundancy clients.

The Media Redundancy Protocol (MRP) is the standard procedure for media redundancy. Using this procedure, a maximum of 50 devices can participate in each ring. In the case of an interrupted cable, data transfer is only briefly interrupted as the system switches over to the redundant data path: This is the reason that the switchover is not bumpless (200 ms).

If a brief interruption is not permitted, then you have the following options

- Correspondingly set the failure monitoring time in the hardware configuration to more than 200 ms.
  or
- Set the data transfer to IRT High Performance.

The uninterruptible MRRT is automatically set. A SIMOTION controller (or another suitable controller) is required in this case.

The two integrated PROFINET IO interfaces of the Control Units CU320-2 PN and CU310-2 PN can be configured as redundancy clients.

From a CBE20, only the first two ports are capable of establishing a ring topology. Routing between the integrated PROFINET IO interfaces and a CBE20 is not possible.

A.1.3.9 PROFINET system redundancy

Thanks to SINAMICS S120 PROFINET Control Unit, the assembly of system-redundant systems is possible.

Precondition for system-redundant systems is a so-called H-system. The H-system consists of 2 fault-tolerant controls – master and reserve CPU – which are constantly synchronized via fiber-optic cables. If one controller fails, the other automatically takes on the job. This reduces system downtimes.

Requirements

- SIMATIC controller S7-400H with two PROFINET H-CPUs type 41xH (or newer: e.g. SIMATIC S7-1500 R/H)
- SINAMICS S120 PROFINET Control Unit (CU310-2 PN or CU320-2 PN)
- Redundant communication links

Benefits

- No system downtime in the case of a controller failure
- Component replacement possible during ongoing operation
- Configuration changes possible during ongoing operation
- Automatic synchronization after replacing components

Restrictions

- IRT is not supported
- No simultaneous operation of Shared Device and Shared I-Device
- Maximum 2 cyclical PROFINET connections
- System redundancy only via the onboard interface of SINAMICS S120 PROFINET Control Unit
- For the duration of switching from one controller to the other, the setpoints of the last connection remain frozen and valid.

Design, configuring and diagnostics

Configuration

The figure below shows a sample structure of a system-redundant controller with 3 converters.

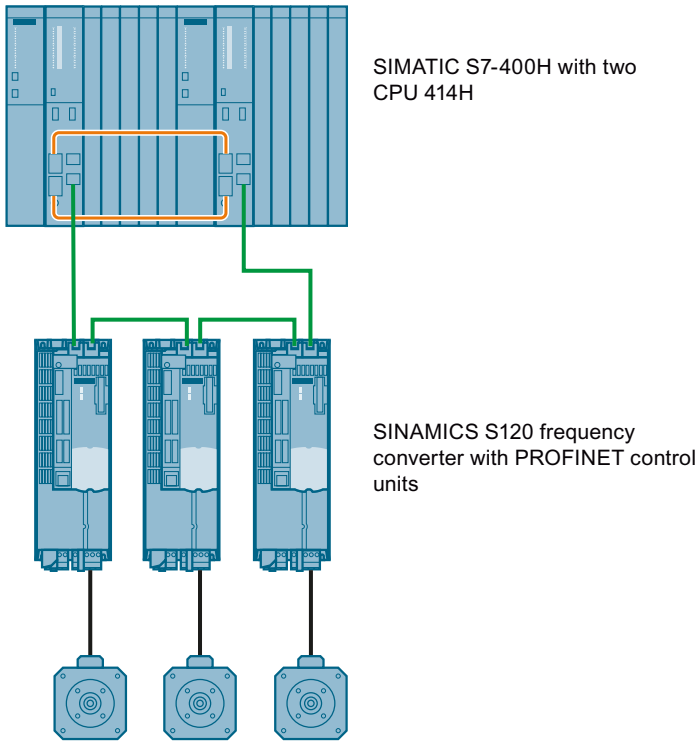


Figure A-46 System redundancy with converters

Configuring

Configuring the redundancy takes place in STEP 7. In the converter, you only have to configure the communication via PROFINET.

System redundancy does not depend on the topology of the system.

Diagnostics LEDs

Diagnostics states are shown as follows using LEDs with PROFINET system redundancy:

Color	State	Significance
Green	Continuous light	2 redundancy connections available and setpoints are OK.
Green	Flashing light	Only one redundancy connection is available or setpoints are missing.
Red	Flashing light 2 Hz	No connection or setpoint failure (F01910).

Additional information

You can find further descriptions of the PROFINET system redundancy online in the following manuals:

- System manual "Fault-tolerant SIMATIC S7-400H systems"
  SIMATICS S7-400H Manual (https://support.industry.siemens.com/cs/ww/en/view/82478488)
- Application description Configuration examples for S7-400H PROFINET
  SIMATICS S7-400H Configuration examples (https://support.industry.siemens.com/cs/ww/en/view/90885106)
- Application example (https://support.industry.siemens.com/cs/de/en/view/109744811)

Messages and parameters

Faults and alarms (see SINAMICS S120/S150 List Manual)

- F01910 (N, A) Fieldbus: Setpoint timeout
- A01980 PN: Cyclic connection interrupted
- A01982 PN: Second controller missing
- A01983 PN: System redundancy switchover running

Overview of important parameters (see SINAMICS S120/S150 List Manual)

- r2043.0...2 BO: IF1 PROFIdrive PZD status
- r8843.0...2 BO: IF2 PZD status
- r8936[0...1] PN state of the cyclic connection
- r8937[0...5] PN diagnostics
- r8960[0...3] PN subslot controller assignment
- r8961[0...3] PN IP Address Remote Controller 1
- r8962[0...3] PN IP Address Remote Controller 2

A.1.3.10 PROFIenergy

PROFIenergy is an energy management system for production plants, based on the PROFINET communication protocol. The functionality is certified in the PROFIenergy profile of the PNO. Drive units which have PROFIenergy functionality, can be certified in an approved laboratory. Certified devices support the PROFIenergy commands and respond accordingly to the requirements and operating states.

SINAMICS supports the PROFIenergy profile V1.1. PROFIenergy commands are acyclically transferred from the controller to the drive with PROFINET data sets. The PROFIenergy commands are transferred using the PROFINET data set 0x80A0.

PROFIenergy data record access is only accepted via the connection types "RT connection" or "IRT connection".

If access is made via another type of connection (e.g. Supervisor connection), system redundancy connection), the data record access is rejected with error code 0x80B0 “Invalid Index”.

There is exactly one PROFIenergy access point (PESAP) and this hangs on the MAP submodule of the CU drive object.

If access is made via another module/submodule, the data record access is rejected with error code 0x80B0 “Invalid Index”.

PROFIenergy properties of the SINAMICS S120 drive system

SINAMICS S120 drive system devices meet the following requirements:

- Are certified for PROFIenergy
- PROFIenergy function unit Class 3
- PROFIenergy energy-saving mode 2

SINAMICS devices support the following PROFIenergy functions:

Functions		SINAMICS support								
		S120 SERVO	S120 VECTOR	S150	G110M	G120D	G120x (otherwise not G120D)	G130	G150	ET200 pro FC-2
Control commands		X	X	X	X	X	X	X	X	X
Query commands		X	X	X	X	X	X	X	X	X
Measured values	ID 34	X	X	X	X	X	X	X	X	X
	ID 166	–	X	X	X	X	X	X	X	X
	ID 200	X	X	X	X	X	X	X	X	X
Measuring value access		X	X	X	X	X	X	X	X	X
PROFIenergy energy-saving mode 1	Shutdown Digital outputs	–	–	–	–	X	–	–	–	–
	Shutdown Encoder	–	–	–	–	X	–	–	–	–
PROFIenergy energy-saving mode 2	Switch on interlocking	X	X	X	X	–	X	X	X	X
Inhibit PROFIenergy		X	X	X	X	X	X	X	X	X
PROFIenergy energy-saving mode in PROFIdrive state S3/S4		–	–	–	X	X	X	X	X	X

Figure A-47 PROFIenergy functions

Tasks of PROFIenergy

PROFIenergy is a data interface based on PROFINET. This data interface allows loads to be shut down during non-operational periods in a controlled fashion, and irrespective of the manufacturer and device. Consequently, the process should be given only the energy it actually requires. The majority of the energy is saved by the process, the PROFINET device itself contributes only a few watts to the saving potential.

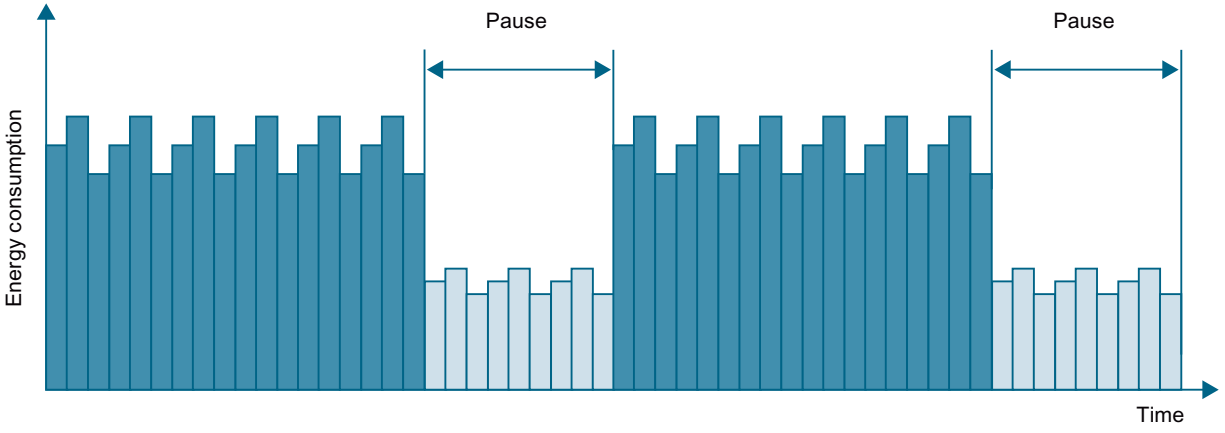


Figure A-48 Energy saving during pauses with PROFIenergy

The following objectives are reached in detail by temporarily shutting down or stopping unused drives and equipment:

- Lower energy costs.
- Reduction of thermal emissions.
- Longer service life by reducing the effective operating times.
- The drive units provide standardized consumption data for analysis.
- The PROFIenergy state of the participating devices is displayed.
- The PROFIenergy state is available with BICO interconnections for further processing, e.g. to shutdown secondary systems that are not required.

Basics

The PROFINET devices and the power modules are shut down using special commands in the user program of the PROFINET IO controller. No additional hardware is required; the PROFIenergy commands are interpreted directly by the PROFINET devices.

PROFIenergy commands

Principle of operation

At the start and end of pauses, the plant operator activates or deactivates the pause function of the plant/system after which the IO controller sends the PROFIenergy "START_Pause" / "END_Pause" command to the PROFINET devices. The device then interprets the content of the PROFIenergy command and switches off or on again.

You can call up device information via additional PROFIenergy functions. You can use these to transfer the "START_Pause"/"END_Pause" command in plenty of time.

PROFIenergy control commands

Control commands	Description
START_Pause	Switches from the operating state to the energy-saving mode depending on the pause duration. Switches from the energy-saving mode to the operating state depending on the pause duration.
START_Pause_with_time_response	Switches from the operating state to the energy-saving mode and also specifies the transition times in the command response.
END_Pause	Switches from the energy-saving mode to the operating state. Cancels a switch from the operating state to the energy-saving mode.

PROFIenergy query commands

Query commands	Description
List_Energy_Saving_Modes	Determines all supported energy-saving modes.
Get_Mode	Determines the energy-saving mode.
PEM_Status	Determines the current PROFIenergy status.
PEM_Status_with_CTTO	Determines the actual PROFIenergy status, the same as for the command "PEM status" and in addition with the regular transition time to the operating state.
PE_Identify	Determines the supported PROFIenergy commands.
Query_Version	Shows the implemented PROFIenergy profile.
Get_Measurement_List	Returns the measured value IDs that can be accessed using the "Get_Measurement_Values" command.
Get_Measurement_List_with_object_number	Returns the measured value IDs and the associated object number that can be accessed using the "Get_Measurement_Values_with_object_number" command.

Query commands	Description
Get_Measurement_Values	Returns the requested measured value using the measured value ID: • For power measured values: The command addresses the sum of the measured value over all control drive objects. • For energy measured values: The command returns the sum of the measured value over all control drive objects. • For power factors: This measured value is supported only for a SINAMICS with a control drive object.
Get_Measurement_Values_with_object_number	Returns the requested measured values using the measured value ID and the object number. The object number corresponds to the drive object ID. The drive object ID of the Control Unit is used to address the measured values as with "Get_Measurement_Value".

PROFIenergy measured values

Table A-17 Overview of the PROFIenergy measured values

PROFIenergy measured value		PROFIenergy accuracy		Unit	SINAMICS source parameters		Value range
ID	Name	Domain	Class		Parameters	Name	
34	Active power	1	12	W	r0032	Active power smoothed	Largest value for r2004 of all drive objects
166	Power factor	1	12	1	r0038	Smoothed power factor	0 ... 1
200	Active energy import	2	11	Wh	r0039[1]	Energy accepted	-

PROFIenergy energy-saving mode

SINAMICS S120 drive devices support PROFIenergy energy-saving mode 2. The following two parameters indicate the effective PROFIenergy mode:

- Parameter r5600 indicates the currently active PROFIenergy mode.
- Using interconnectable bits, the r5613 parameter indicates whether the PROFIenergy energy saving is active.

Activating the energy-saving mode

The energy-saving mode can activated or deactivated using the PROFIenergy control commands (see also PROFIenergy commands (Page 181)).

General converter behavior when in the PROFIenergy energy-saving mode

- When the PROFIenergy energy-saving mode is active, the converter issues alarm A08800.
- When the PROFIenergy energy-saving mode is active, the converter does not send any diagnostic alarms.
- If the PROFIenergy energy-saving mode is active, then the READY LED flashes green in the on / off ratio: 500 ms on, 3000 ms off.
- If the bus connection to the control system is interrupted while the converter is in the energy-saving mode, the converter exits the energy-saving mode and resumes normal operation ("ready_to_operate").
- The converter changes into normal operation if the control system goes into the stop condition while the converter is in the energy-saving mode.

PROFIenergy inhibit and pause time

Block PROFIenergy

If you set p5611.0 = 1, you inhibit the response of the inverter to PROFIenergy control commands. In this case, the converter ignores the PROFIenergy control commands.

Pause time

- Minimum pause time: p5602
  - When the pause time, which is sent using command "Start_Pause", is equal to or greater than the value in p5602[1], then the inverter goes into the energy-saving mode.
  - If the pause time is less than p5602[1], the inverter ignores the command.
- Maximum duration: p5606

Function diagrams and parameters

Function diagrams (see SINAMICS S120/S150 List Manual)

- 2381 PROFIenergy - Control commands / query commands
- 2382 PROFIenergy - States
- 2610 Sequence control - Sequencer

Overview of important parameters (see SINAMICS S120/S150 List Manual)

- r5600 Pe hibernation ID
- p5602[0...1] Pe hibernation pause time, minimum
- p5606[0...1] Pe hibernation duration, maximum
- p5611 Pe energy-saving properties, general
- r5613.0...1 CO/BO: Pe energy-saving active/inactive

A.1.3.11 Messages via diagnostics channels

Messages are not just able to be displayed via the Startdrive commissioning tools. After the activation of a diagnostic function, the messages are also transferred to the higher-level controller via the standardized diagnostic channels. The messages are evaluated there or forwarded for convenient display to the corresponding user interfaces (SIMATIC HMI, TIA Portal, etc.).

In this way, problems or faults can be located immediately regardless of the tool currently being used, and then corrected immediately.

Also note the general information on the diagnostics channels in Section Diagnostics channels (Page 98).

Activating the diagnostic function

The diagnostics function is activated or deactivated via the parameterization of the relevant configuration tool (HW Config, TIA Portal, etc.).

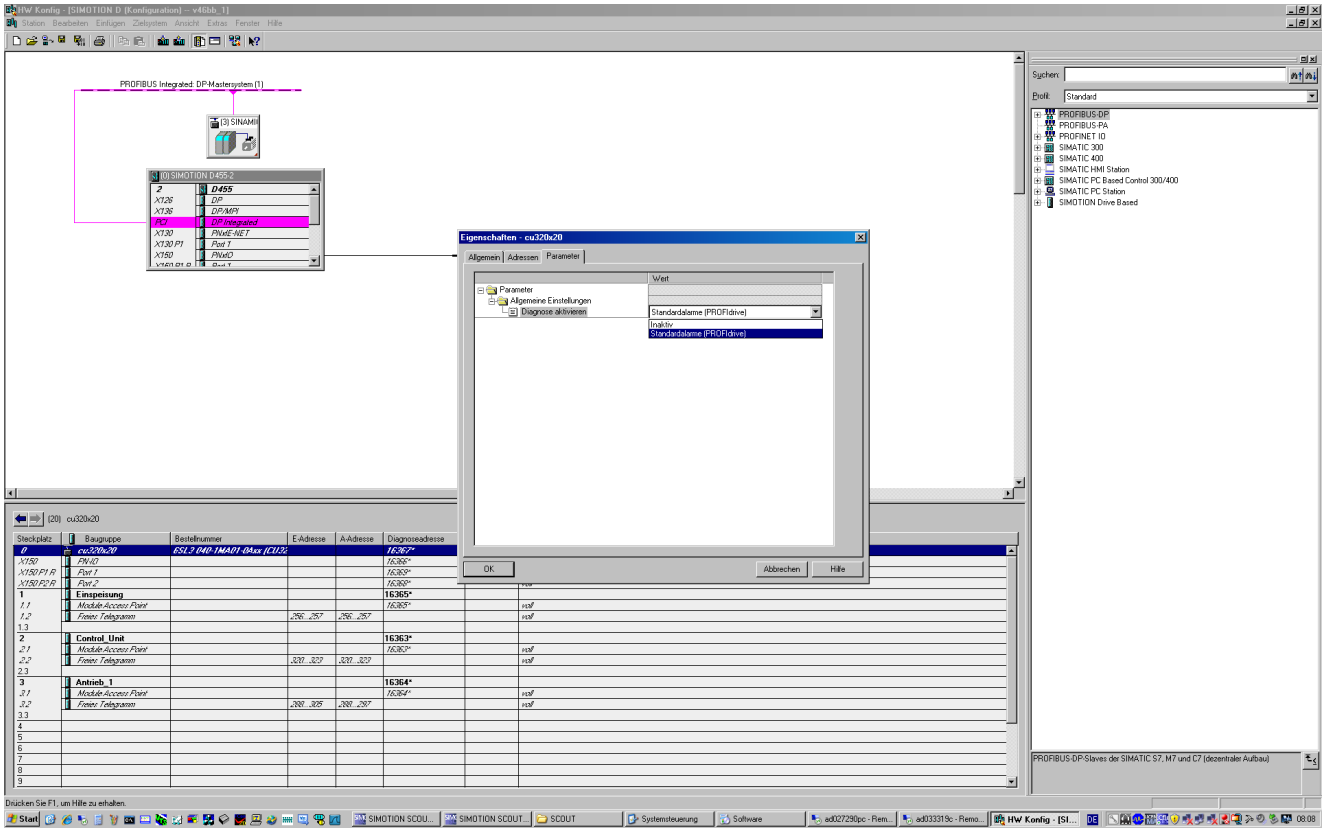


Figure A-49 Activation of PROFINET

The following parameter assignments are possible:

Setting	Code for parameter assignment
Inactive	0
PROFIdrive error classes	1

When establishing the communication between SINAMICS and a controller, the activated diagnostics mode of this controller is first transferred to the drive. With activated diagnostics, SINAMICS first transfers all pending messages to the controller. Similarly, all currently active messages in the controller are deleted by SINAMICS when closing the communication connection.

Messages

The message texts are described in detail in the SINAMICS S120/S150 List Manual, Chapter "Explanations on the list of faults and alarms". A current list of the message texts can be found in the "Message classes and coding of different diagnostics interfaces" table.

A.1.3.12 Support of I&M data sets 1...4

Identification & Maintenance (I&M)

I&M data sets contain information for a standardized and simplified identification and maintenance of PROFIBUS/PROFINET devices. I&M data sets 1...4 contain plant-specific information, such as the installation location and date. PROFINET supports I&M data sets 0...4.

I&M data sets 1...3 can be set with the SIMATIC Manager (STEP 7) and also with HW Config (STEP 7).

The I&M data sets 1...4 are permanently stored in parameters p8806...p8809. Essential properties of these 3 parameters:

- They can be listed in the Startdrive "Parameter list".
- The SINAMICS "Reset parameter" (p0976 = 1, p0970 = 1) function does not have any effect on the content of the parameters.
- I&M data sets are not changed when the alternative parameter sets are stored or loaded. The transfer of parameter sets between a memory card and non-volatile device memory does not have any effect on the I&M data sets.

Overview of important parameters (see SINAMICS S120/S150 List Manual)

- p8806[0...53] Identification and Maintenance 1
- p8807[0...15] Identification and Maintenance 2
- p8808[0...53] Identification and Maintenance 3
- r8809[0...53] Identification and Maintenance 4

I&M parameters

Table A-18 Parameter designation, assignment and meaning

I&M parameter designation	Format	Size/ octets	Initialization	SINAMICS parameters	Meaning
I&M 1: TAG_FUNCTION	Visible string	32	Space 0x20... 0x20	p8806[0...31]	Text that identifies the function or task of the device.
I&M 1: TAG_LOCATION	Visible string	22	Space 0x20... 0x20	p8806[32...53]	Text that identifies the device location.

I&M parameter designation	Format	Size/ octets	Initialization	SINAMICS parameters	Meaning
I&M 2: INSTALLATION_DATE	Visible string	16	Space 0x20... 0x7E	p8807[0...15]	Text with the date of the installation or the initial commissioning of the device. The following date formats are supported: • YYYY-MM-DD • YYYY-MM-DD hh:mm – YYYY: Year – MM: Month 01...12 – DD: Day 01...31 – hh: Hours 00...23 – mm: Minutes 00...59 The separators between the individual specifications, i.e. hyphen '-', blank ' ' and colon ':', must be entered.
I&M 3: DESCRIPTOR	Visible string	54	Space 0x20... 0x20	p8808[0...53]	Text with any comments or notes.
I&M 4: SIGNATURE	Octet string	54	Space 0x00... 0x00	r8809[0...53]	The parameter is automatically populated by the system, in which case it contains a functional check signature for the change tracking with Safety Integrated. The check signature has the following format: • The first four octets (0...3) contain the content of parameter r9781 index 0: "SI change monitoring checksum (Control Unit)". • The second four octets (4...7) contain the content of parameter r9782 index 0: "SI change monitoring time stamp (Control Unit)". • The remainder (octets 8...53) contains zeroes.

A.1.4 Communication via Modbus TCP

The Modbus protocol is a communication protocol based on a controller/device architecture.

Modbus offers three transmission modes:

- **Modbus ASCII -** via a serial interface
  data in the ASCII code. The data throughput is lower compared to RTU.
- **Modbus RTU** - via a serial interface
  data in the binary format. The data throughput is greater than in ASCII code.
- **Modbus TCP -** via Ethernet
  data as TCP/IP packages. TCP port 502 is reserved for Modbus TCP.

Only transfer type "Modbus TCP" is available for SINAMICS S120.

Possible drive units:

- CU320-2 PN
- CU320-2 DP (CBE20)
- CU310-2 PN

Modbus functionality

Process data and parameters are accessed via the Modbus register.

- Process data: 40100 - 40119
- Drive data: 40300 - 40522
- All parameters via DS47: 40601 - 40722

Modbus TCP always provides a basic Ethernet functionality, which corresponds to the functionality of Ethernet interface X127:

- Commissioning access for Startdrive with the S7 protocol
- DCP to set the IP address etc.
- SNMP for identification

General information about communication

Communication with Modbus TCP is established via the Ethernet/PROFINET interfaces:

- **X150**
  For Modbus TCP with a CU320-2 PN or CU310-2 PN.
- **X1400**
  For Modbus TCP with a CU320-2 PN or a CU320-2 DP via a CBE20.

Precisely one Modbus connection can be established. A simultaneous connection via the interfaces X150 and X1400 is not possible and is acknowledged with alarm A08555(1).

However, you can use one interface for Modbus TCP, and the other as PROFINET interface.

Drive object that can be addressed via Modbus

With Modbus TCP, you always address the first control-drive object from the list of drive objects (p0978[0]). A servo or vector drive object must be in this parameter.

- However, Modbus TCP is only activated if, under p0978[0], there is a drive object that is supported by Modbus TCP.
- If p0978[0] does not contain a valid drive object, then establishing communication is acknowledged with alarm A08555(2).

Diagnostics LEDs in Modbus TCP

Diagnostics states are shown as follows using LEDs with Modbus TCP:

- X150: "**PN**" LED
- X1400 (CBE20): "**OPT**" LED

The following states can be displayed by these LEDs:

Color	State	Meaning
Green	Continuous light	Connections and setpoints are OK.
Green	Flashing light	Connection is OK, but no setpoints (dependent on timeout).
Red	Flashing light 2 Hz	No connection or setpoint timeout.

A.1.4.1 Configuring Modbus TCP via interface X150

Activate Modbus TCP via X150 (CU320-2 PN or CU310-2 PN)

1. For drive object DO1, set p2030 = 13 (Modbus TCP).
2. Using p8921, set the IP address for the onboard PROFINET interface on the Control Unit.
3. Set the standard gateway using p8922.
4. Set the subnet mask using p8923.
5. Set the DHCP mode using p8924.
6. Select "Activate and save configuration" as interface configuration using p8925 = 2.
7. In the Startdrive commissioning tool, check the list of drive objects p0978.
   When required, change the sequence of the drive objects using the telegram configuration ("Drive device" > "Communication" > "Telegram configuration").
8. Save the settings in the Startdrive commissioning tool and carry out a POWER ON.

Modbus settings with interface X150

Using the following parameters, set the communication for Modbus TCP with a X150 interface:

Parameters	Explanation
p2040	Setting the monitoring time to monitor the received process data via fieldbus interface. If process data is not transferred within one cycle of the fieldbus monitoring time, then the drive shuts down with fault F01910.
r2050[0...19]	Connector output to interconnect the PZD received from the fieldbus controller via IF1.
p2051[0...24]	Selects the PZD (actual values) to be sent to the fieldbus controller in the word format via IF1.
r2053[0...24]	Displays the PZD (actual values) sent to the fieldbus controller in the word format via IF1.
r2054	Status display for the internal communication interface.
p8839[0...1]	Assigning the PN onboard interface (x150) via PZD interface 1 (IF1) and interface 2 (IF2).
r8850[0...19]	Connector output to interconnect the PZD (setpoints) received in the word format via IF2.
p8851[0...24]	Selects the PZD (actual values) to be sent in the word format via IF2.
r8853[0...24]	Displays the PZD (actual values) sent in the word format via IF2.
r8854	Status display for COMM BOARD.

A.1.4.2 Configuring Modbus TCP via interface X1400

Activating Modbus TCP via X1400 (CBE20)

1. For drive object DO1, set p8835 = 5 (Modbus TCP).
2. Set the IP address for the CBE20 using p8941.
3. Set the standard gateway for the CBE20 using p8942.
4. Set the subnet mask for the CBE20 using p8943.
5. Set the DHCP mode for the CBE20 using p8944.

6. Select the setting "Activate and save configuration" as interface configuration using p8945 = 2.
7. In the Startdrive commissioning tool, check the list of drive objects p0978.
   When required, change the sequence of the drive objects using the telegram configuration ("Drive device" > "Communication" > "Telegram configuration").
8. Save the settings in the Startdrive commissioning tool and carry out a POWER ON.

Modbus settings with interface X1400

Using the following parameters, set the communication for Modbus TCP with a X1400 interface:

Parameters	Explanation
r2050[0...19]	Connector output to interconnect the PZD received from the fieldbus controller via IF1.
p2051[0...24]	Selects the PZD (actual values) to be sent to the fieldbus controller in the word format via IF1.
r2053[0...24]	Displays the PZD (actual values) sent to the fieldbus controller in the word format via IF1.
r2054	Status display for the internal communication interface.
p8840	Setting the monitoring time to monitor the received process data via the COMM BOARD. If, within this time, the Control Unit does not receive any process data from the COMM BOARD, then the drive shuts down with fault F08501.
p8839[0...1]	Assigning the CBE20 interface (x1400) for cyclic communication via PZD interface 1 (IF1) and interface 2 (IF2).
r8850[0...19]	Connector output to interconnect the PZD (setpoints) received in the word format via IF2.
p8851[0...24]	Selects the PZD (actual values) to be sent in the word format via IF2.
r8853[0...24]	Displays the PZD (actual values) sent in the word format via IF2.
r8854	Status display for COMM BOARD.

A.1.4.3 Mapping tables

Modbus register and Control Unit parameters

The Modbus protocol contains register or bit numbers for addressing memory. You must assign the appropriate control words, status words, and parameters to these registers in the device.

The valid holding register address range extends from 40001 up to 40722. When trying to access other holding registers, the "Exception code" error is output

The process data are transferred into the register range from 40100 up to 40119.

Assigning the Modbus register to the parameters - process data

Table A-19 Assigning the Modbus register to the parameters - process data

Register	Description	Access[1)]	Unit	Scaling	ON/OFF text or Value range	Data / parameter
Control data						
40100	Control word (see SINAMICS S120/150 List Manual, function diagram 2442)	R/W	-	1	-	Process data 1

Register	Description	Access[1)]	Unit	Scaling	ON/OFF text or Value range	Data / parameter
40101	Main setpoint	R/W	-	1	-	Process data 2
40102	STW 3	R/W	-	1	-	Process data 3
40103	STW 4	R/W	-	1	-	Process data 4
40104	PZD 5	R/W	-	1	-	Process data 5
40105	PZD 6	R/W	-	1	-	Process data 6
40106	PZD 7	R/W	-	1	-	Process data 7
40107	PZD 8	R/W	-	1	-	Process data 8
40108	PZD 9	R/W	-	1	-	Process data 9
40109	PZD 10	R/W	-	1	-	Process data 10
Status data						
40110	Control word (see SINAMICS S120/150 List Manual, function diagram 2452)	R	-	1	-	Process data 1
40111	Main actual value	R	-	1	-	Process data 2
40112	ZSW 3	R	-	1	-	Process data 3
40113	ZSW 4	R	-	1	-	Process data 4
40114	PZD 5	R	-	1	-	Process data 5
40115	PZD 6	R	-	1	-	Process data 6
40116	PZD 7	R	-	1	-	Process data 7
40117	PZD 8	R	-	1	-	Process data 8
40118	PZD 9	R	-	1	-	Process data 9
40119	PZD 10	R	-	1	-	Process data 10

[1)] "R"; "W"; "R/W" in the “Access" column stands for read (with FC03); write (with FC06); read/write.

Assigning the Modbus register to the parameters - parameter data

Table A-20 Assigning the Modbus register to the parameters - parameter data

Register	Description	Access[4)]	Unit	Scaling	ON/OFF text or Value range	Data / parameter
Drive identification						
40300	Actual power unit code number	R	-	1	0 ... 65535	r0200
40301	Control Unit firmware	R	-	1	0 ... 65535	r0018 / 10000
Drive data						
40320	Rated power of the power unit	R	kW	100	0 ... 655.35	r0206
40321	Current limit	R/W	%	10	0.0 ... 6553.5	p0640
40322	Ramp-up time [1)]	R/W	s	100	10.00 ... 655.35	p1120
40323	Ramp-down time[1)]	R/W	s	100	10.00 ... 655.35	p1121
40324	Reference speed[2)]	R/W	RPM	1	6 ... 65535	p2000
Drive diagnostics						
40340	Speed setpoint[2)]	R	RPM	1	-32768 ... 32767	r0020
40341	Speed actual value[2)]	R	RPM	1	-32768 ... 32767	r0021
40342	Output frequency	R	Hz	100	- 327.68 ... 327.67	r0024

Register	Description	Access[4]	Unit	Scaling	ON/OFF text or Value range	Data / parameter
40343	Output voltage	R	V	1	0 ... 65535	r0025
40344	DC link voltage	R	V	1	0 ... 65535	r0026
40345	Actual current value	R	A	100	0 ... 655.35	r0027
40347	Actual active power	R	kW	100	0 ... 655.35	r0032
40349	Control priority	R	-	1	HAND AUTO	r0807
Fault diagnostics						
40400	Failure number, index 0	R	-	1	0 ... 65535	r0947 [0]
40401	Failure number, index 1	R	-	1	0 ... 65535	r0947 [1]
40402	Failure number, index 2	R	-	1	0 ... 65535	r0947 [2]
40403	Fault number, index 3	R	-	1	0 ... 65535	r0947 [3]
40404	Fault number, index 4	R	-	1	0 ... 65535	r0947 [4]
40405	Fault number, index 5	R	-	1	0 ... 65535	r0947 [5]
40406	Fault number, index 6	R	-	1	0 ... 65535	r0947 [6]
40407	Fault number, index 7	R	-	1	0 ... 65535	r0947 [7]
40408	Alarm number	R	-	1	0 ... 65535	r2110 [0]
40409	Actual alarm code	R	-	1	0 ... 65535	r2132
40499	PRM ERROR code	R	-	1	0 ... 255	-
Technology controller[3]						
40500	Technology controller enable	R/W	-	1	0 ... 1	p2200, r2349.0
40501	Technology controller MOP	R/W	%	100	-200.0 ... 200.0	p2240
Adapt technology controller[3]						
40510	Time constant for actual-value filters of the technology controller	R/W	-	100	0.00 ... 60.0	p2265
40511	Scaling factor for actual value of the technology controller	R/W	%	100	0.00 ... 500.00	p2269
40512	Proportional amplification of the technology controller	R/W	-	1000	0.000 ... 65.535	p2280
40513	Integral time of the technology controller	R/W	s	1	0 ... 60	p2285
40514	Time constant D-component of the technology controller	R/W	-	1	0 ... 60	p2274
40515	Max. limit of technology controller	R/W	%	100	-200.0 ... 200.0	p2291
40516	Min. limit technology controller	R/W	%	100	-200.0 ... 200.0	p2292
PID diagnostics						
40520	Effective setpoint acc. to internal technology controller MOP ramp-function generator	R	%	100	-100.0 ... 100.0	r2250
40521	Actual value of technology controller after filter	R	%	100	-100.0 ... 100.0	r2266
40522	Output signal technology controller	R	%	100	-100.0 ... 100.0	r2294

[1] For these registers, for S120 servo drives, parameters p1120 and p1121 are only available (and can only be parameterized) with the extended setpoint channel.

[2] These registers are not supported for linear motors as the unit and value range differ from normal rotary drives.

[3] You can only access the technology controller parameters if the "Technology controller" function module is also activated.

4) "R"; "W"; "R/W" in the "Access" column stands for read (with FC03); write (with FC06); read/write.

Assigning the Modbus register for general parameter access using DS4

Table A-21 Assignment of the Modbus register for general parameter access using DS47

Register	Description	Access[1)]	Unit	Scaling	ON/OFF text or Value range	Data / parameter
40601	DS47 Control	R/W	-	-	-	-
40602	DS47 header	R/W	-	-	-	-
40603	DS47 data 1	R/W	-	-	-	-
...	...					
40722	DS47 data 120	R/W	-	-	-	-

1) "R"; "W"; "R/W" in the “Access" column stands for read (with FC03); write (with FC06); read/write.

Note

Limited value range

Modbus TCP registers have a maximum 16 bit width. The values of display parameters (r parameters) cannot always be represented with 16 bits. In these particular cases, the maximum value that can be represented is displayed.

- Unsigned: 65535
- Signed min: -32768
- Signed max: 32767

A.1.4.4 Write and read access using function codes

Function codes used

For data exchange between the controller and device, predefined function codes are used for communication via Modbus.

The Control Unit uses the following Modbus function codes:

- FC 03: Holding register to read data from the inverter
- FC 06: Write single register to write to individual register
- FC 16: Write to multiple registers to write to several registers

Structure of a Modbus TCP message

Application Data Unit (ADU)					
Modbus Application Header				Protocol Data Unit (PDU)	
Transaction ID	Protocol ID	Length	Unit ID	FCode	Data
2 Bytes	2 Bytes	2 Bytes	1 Byte	1 Byte	0 ... 252 Bytes

Figure A-50 Individual components, including Modbus Application Header (MBAP) and function code

Structure of a read request via Modbus function code 03 (FC 03)

Any valid register address is permitted as the start address.

Via FC 03, the control can address more than one register with one request. The number of addressed registers is contained in bytes 10 and 11 of the read request.

Table A-22 Structure of a read request for device number 17, example

Value	Byte	Description
MBAP header		
03 h	7	
00 h	8	Register start address "High" (register 40110)
6D h	9	Register start address "Low"
00 h	10	Number of registers "High" (2 registers: 40110; 40111)
02 h	11	number of registers "Low"

The response returns the corresponding data set:

Table A-23 Device response to the read request, example

Value	Byte	Description
MBAP header		
03 h	7	
04 h	8	Number of bytes (4 bytes are returned)
11 h	9	Data first register "High"
22 h	10	Data first register "Low"
33 h	11	Data second register "High"
44 h	12	Data second register "Low"

Table A-24 Invalid read request

Read request	Converter response
Invalid register address	Exception code 02 (invalid data address)
Read a write-only register	Telegram in which all values are set to 0.
Read a reserved register	
Controller addresses more than 125 registers	Exception code 03 (invalid data value)
The start address and the number of registers of an address are located outside of a defined register block	Exception code 02 (invalid data address)

Structure of a write request via Modbus function code 06 (FC 06)

Start address is the holding register address.

Via FC 06, with one request, only precisely one register can be addressed. The value, which is written to the addressed register, is contained in bytes 10 and 11 of the write request.

Structure of a write request for device number 17, example		
Value	**Byte**	**Description**
MBAP header		
06 h 00 h 63 h 55 h 66 h	7 8 9 10 11	Function code Register start address "High" (write register 40100) Register start address "Low" Register data "High" Register data "Low"
The response returns register address (bytes 8 and 9) and the value (bytes 10 and 11), which the higher-level control had written to the register.		

Device response to the write request, example		
Value	**Byte**	**Description**
MBAP header		
06 h 00 h 63 h 55 h 66 h	7 8 9 10 11	Function code Register start address "High" Register start address "Low" Register data "High" Register data "Low"

Invalid write request	
Write request	**Converter response**
Incorrect address (a holding register address does not exist)	Exception Code 02 - invalid data address
Write in a "read-only" tab	Exception Code 04 - device failure
Write to a reserved register	
For Exception Code 4, via the holding register 40499, you can read out the internal drive error code, which has occurred for the last parameter access via the holding register.	

A.1.4.5 Communication via data set 47

Via FC 16, with one request, up to 122 registers can be written to directly one after the other, while for Write Single Register (FC 06) you must individually write the header data for each register.

Header

In addition to the transfer type, the start address and the number of the following registers in the header.

User data

You control the access in the user data via register 40601.

In register 40602, you define the access as well as the length of the request data.

Register 40603 contains the request reference - it is defined by the user - and the access type - reading or writing.

From register 40603 and higher, the request aligns communication via data set 47 according to PROFIdrive.

Register 40604 contains the number of the drive object and the number of parameters that are read out or written to.

Register 40605 contains the attribute that you use to control whether you read out the parameter value or the parameter attribute. In the number of elements you specify how many indices are read.

Communication details

General parameter access is realized using the Modbus register 40601 ... 40722.

Communication via DS47 is controlled using 40601. 40602 contains the function code (always = 47 = 2F hex) and the number of the following user data. User data are contained in registers 40603 ... 40722.

Communication overview

Value in the register				Explanation
40601	**40602**		**40603 ... 40722**	
0	47	...	...	Write values for acyclic access
1	47	Request length [bytes]	Request data	Activate acyclic access
2	47	Response length [bytes]	Response data	Response for a successful request
2	47	0	Error code	Response for an erronous request

Error codes

1 hex: Invalid Length (invalid length)
2 hex: Invalid State (in the actual inverter state, this action is not permitted)
3 hex: Invalid function code (FC ≠ 2F hex)
4 hex: Response not ready (the response has still not been issued)
5 hex: Internal Error (general system error)

Incorrect access operations to parameters via data set 47 are logged in registers 40603 ... 40722. The error codes are described in the PROFIdrive profile.

Examples: Read parameter

Write parameter request: Reading parameter value of r0002 from device number 17

Table A-25 Write parameter request: Reading parameter value of r0002 from device number 17

Value	Byte	Description
MBAP header		
0010 h	7	Function code (Write multiple)
0258 h	8,9	Start address tab
0007 h	10,11	Number of registers to be read (40601 … 40607)
000E h	12	Number of data bytes (7 registers, each 2 bytes = 14 bytes)
0001 h	13,14	40601: DS47 Control = 1 (activate request)
2F0A h	15,16	40602: Function code 2F h (47), request length 10 bytes (0A h)
8001 h	17,18	40603: Request reference = 80 h, request identifier = 1 h
0101 h	19,20	40604: DO-ID = 1, number of parameters = 1
1001 h	21,22	40605: Attribute, number of elements = 1
0002 h	23,24	40606: Parameter number = 2
0000 h	25,26	40607: Subindex = 0

Start parameter request: Reading parameter value of r0002 from device number 17

Table A-26 Start parameter request: Reading parameter value of r0002 from device number 17

Value	Byte	Description
MBAP header		
0003 h	7	Function code (read)
0258 h	8,9	Start address tab
0007 h	10,11	Number of registers to be read (40601 … 40607)
0010 h	12,13	Number of registers

Response for successful read operation

Table A-27 Response for successful read operation

Value	Byte	Description
MBAP header		
0003 h	7	Function code (read)
0020 h	8	Number of following data bytes (20 h: 32 bytes ≙ 16 registers)
0002 h	9,10	40601: DS47 Control = 2 (the request was executed)
2F08 h	11,12	40602: Function code 2F h (47), response length 8 bytes
8001 h	13,14	40603: Request reference mirrored = 80 h, Response = 1 (request parameter)
0101 h	15,16	40604: DO-ID = 1, number of parameters = 1
0301 h	17,18	40605: Format, number of elements = 1
001F h	19,20	40606: Parameter value = 1F h (31)

Response for unsuccessful read operation - read request still not completed

Table A-28 Response for unsuccessful read operation - read request still not completed

Value	Byte	Description
MBAP header		
0003 h 0020 h	7 8	Function code (read) Number of following data bytes (20 h: 32 bytes ≙ 16 registers)
0001 h 2F00 h 0004 h	9,10 11,12 13,14	40601: Check value 1 = request is processed 40602: Function 2F h(47), response length 0 (fault) 40603: Error code: 0004 Response Not Ready (response has still not been issued)

Examples: Write parameter

Write parameter request: Writing the parameter value of p1121 from device number 17

Table A-29 Write parameter request: Writing the parameter value of p1121 from device number 17

Value	Byte	Description
MBAP header		
0010 h 0258 h 000A h 0014 h	7 8,9 10,11 12	Function code (Write multiple) Start address tab Number of registers to be written (40601 … 40610) Number of data bytes (10 registers, each 2 bytes = 20 bytes)
0001 h 2F10 h 8002 h 0101 h 1001 h 0461 h 0000 h 0801 h 4142 h 6666 h	13,14 15,16 17,18 19,20 21,22 23,24 25,26 27,28 29,30 31,32	40601: C1 (activate request) 40602: Function code 2F h (47), request length 16 bytes (10 h) 40603: Request reference = 80 h, request identifier = 2 h (write) 40604: DO-ID = 1, number of parameters = 1 40605: Attribute, number of elements = 1 40606: Parameter number = 1121 40607: Subindex = 0 40608: Format + number of values 40609: Parameter value 12,15 40610: Parameter value

Start parameter request: Writing the parameter value of p1121 from device number 17

Table A-30 Start parameter request: Writing the parameter value of p1121 from device number 17

Value	Byte	Description
MBAP header		
0003 h 0258 h 0007 h 0010 h	7 8,9 10,11 12,13	Function code (read) Start address tab Number of registers to be written (40601 … 40610) Number of registers

Response for successful write operation

Table A-31 Response for successful write operation

Value	Byte	Description
MBAP header		
0003 h 0020 h	7 8	Function code (read) Number of following data bytes (20 h: 32 bytes ≙ 16 registers)
0002 h 2F04 h 8002 h 0101 h	9,10 11,12 13,14 15,16	40601: DS47 Control = 2 (the request was executed) 40602: Function code 2F h (47), response length 4 bytes 40603: Request reference mirrored = 80 h, Response = 2 (change parameter) 40604: DO-ID = 1, number of parameters = 1

Response for unsuccessful write operation - write request still not completed

Table A-32 Response for unsuccessful write operation - write request still not completed

Value	Byte	Description
MBAP header		
0003 h 0020 h	7 8	Function code (read) Number of following data bytes (20 h: 32 bytes ≙ 16 registers)
0001 h 2F00 h 0004 h	9,10 11,12 13,14	40601: DS47 Control = 1 (request is processed) 40602: Function 2F h(47), response length 0 (fault) 40603: Error code: 0004 Response Not Ready (response has still not been issued)

A.1.4.6 Communication procedure

Logical error

If the device detects a logical error within a request, it responds to the controller with an "exception response". In the response, the device sets the highest bit in the function code to 1. If the device receives, for example, an unsupported function code from the controller, the device responds with an "exception response" with code 01 (illegal function code).

Table A-33 Overview of exception codes

Exception code	Modbus name	Remark
01	Illegal function code	An unknown (unsupported) function code was sent to the device.
02	Illegal Data Address	An invalid address was requested.
03	Illegal data value	An invalid data value was detected.
04	Server failure	The device terminated during processing.

Process data monitoring time (setpoint timeout)

The "Setpoint timeout" only applies for access to process data (40100 ... 40109, 40110 ... 40119). The "Setpoint timeout" is not generated for parameter data (40300 ... 40522).

Fieldbus interface:

In parameter p2040 you define the time for cyclic data exchange for process data.

Setting range 0 - 2000 s.

The time depends on the amount of data to be transferred and the control.

"Setpoint timeout" (F01910) is issued by the Modbus if p2040 is set to a value > 0 ms and no process data is requested within this time period.

COMM BOARD:

In parameter p8840 you define the time for cyclic process data exchange.

Setting range 0 - 2000 s.

The time depends on the amount of data to be transferred and the control.

"Setpoint timeout" (F08501) is issued by the Modbus if p8840 is set to a value > 0 ms and no process data is requested within this time period.

A.1.4.7 Messages and parameters

Faults and alarms (see SINAMICS S120/S150 List Manual)

- F01910 Fieldbus: Setpoint timeout
- A01925 (F) Modbus TCP connection interrupted

- F08501 (N, A) PN/COMM BOARD: Setpoint timeout
- A08526 (F) PN/COMM BOARD: No cyclic connection
- A08555 Modbus TCP commissioning fault

Overview of important parameters (see SINAMICS S120/S150 List Manual)

- p0978[0...n] List of drive objects
- p2030 Fieldbus interface protocol selection
- p2040 Fieldbus interface monitoring time:
- r2050[0...19] CO: IF1 PROFIdrive PZD receive word
- p2051[0...24] CI: IF1 PROFIdrive PZD send word
- r2053[0...24] IF1 PROFIdrive diagnostics PZD send word
- r2054 PROFIBUS status
- p8835 CBE20 firmware selection
- p8839[0...1] PZD interface hardware assignment
- p8840 COMM BOARD monitoring time
- r8850[0...19] CO: IF2 PZD receive word
- p8851[0...24] CI: IF2 PZD send word
- r8853[0...24] IF2 diagnostics PZD send
- r8854 COMM BOARD state
- p8920[0...239] PN Name of Station
- p8921[0...3] PN IP address
- p8922[0...3] PN default gateway
- p8923[0...3] PN Subnet Mask
- p8924 PN DHCP mode
- p8925 PN interfaces configuration
- p8940[0...239] CBE2x Name of Station
- p8941[0...3] CBE2x IP address
- p8942[0...3] CBE2x Default Gateway
- p8943[0...3] CBE2x Subnet Mask
- p8944 CBE2x DHCP mode
- p8945 CBE2x interfaces configuration

A.1.5 Communication via Ethernet/IP (EIP)

EtherNet/IP (EIP) is a realtime Ethernet, and is mainly used in automation technology.

The EtherNet Industrial Protocol (EtherNet/IP) is an open standard for industrial networks. EtherNet/IP is used to transmit cyclic I/O data and acyclic parameter data. EtherNet/IP was developed by Rockwell Automation and the Open Device-Net Vendor Association (ODVA (https://www.odva.org/Technology-Standards/EtherNet-IP/Overview)), and standardized in the series of international IEC 61158 standards. EtherNet/IP uses the basis technology of Ethernet TCP/IP, which has been well proven in practice. Ethernet twisted-pair cables or fiber-optic cables are

used as data transmission medium. The CIP protocol (Common Industrial Protocol) – known from DeviceNet and ControlNet – is used as application protocol.

General information about communication

Communication via EIP requires the following interfaces:

- The Ethernet interface (X1400) of the Ethernet CBE20 option board
- The onboard PROFINET interface (X150) at the CU320-2 PN and CU310-2 PN Control Units

The interfaces are either individually available at the different Control Units, or together at one Control Unit (e.g. at a CU320-2 PN with CBE20).

The following table provides an overview of the configurable Control Units and interfaces that are available for communication via EIP.

Table A-34 Configurable Control Units and interfaces

Control Unit	EIP via X150	EIP via X1400 (CBE20)
CU320-2 PN	Yes	No
CU320-2 PN with CBE20 (optional)	Yes	Yes
CU310-2 PN	Yes	No
CU320-2 DP with CBE20	No	Yes

Independent of the configuration, only one interface can be assigned for communication via EIP. A simultaneous connection via the interfaces X150 and X1400 is not possible and is acknowledged with alarm A08555(1).

A.1.5.1 Connecting the drive device to EIP

In order that your drive can be connected to a control system via EIP, your control system requires a generic I/O module for cyclic communication via EIP. You manually create this generic I/O module in the control system.

Create generic I/O module and connect the drive to the control system

To connect the drive to a control system via EIP, proceed as follows:

1. Connect the drive to the control system via an Ethernet cable.
2. In your control system, create a generic I/O module with EIP functionality.
   - Insert a new module in your control system.
   - Select a generic Ethernet module from the selection.
   - Enter the network parameters for the newly inserted module (IP address, subnet mask, standard gateway, station name).

3. For the generic I/O module, enter the lengths of the process data for cyclic communication, which you have selected in Startdrive, r2067[0] (input), r2067[1] (output), for example: Standard telegram 2/2.
   In the Startdrive telegram configuration, read out the length of the process data for all drive objects (for input and output) - and add them (see PROFIdrive "Process data (Page 72)").
   - Input 101:
     Here, enter the sum of all input process data of your drive objects from Startdrive.
   - Output 102:
     Here, enter the sum of all output process data of your drive objects from Startdrive.
   - Configuration 1 or 103:
     Here, always enter a value of 0.
   - 4 ms is supported as the minimum value for RPI (Requested Packet Interval).
4. In Startdrive, set the same values for IP address, subnet mask, standard gateway and the name station as in the control system (see Chapter "Configuring EIP via the onboard PROFINET X150 interface (Page 206)")

Result:

You have connected the drive to the control system via EIP.

Further, you can find a detailed description of how to create a generic I/O module on the following Internet page:
(Gen_Module (https://support.industry.siemens.com/cs/ww/en/view/92045369)).

Routing and shielding Ethernet cables

You can find information on how to do this on the Internet page of "Open Device-Net Vendor Association (ODVAODVA (https://www.odva.org/Publication-Download))".

Commissioning the drive in an EIP network

To commission the drive, connect the drive via an interface (depending on the Control Unit type: PROFIBUS, PROFINET, Ethernet, etc.) with your computer on which Startdrive is installed.

You can find additional information in the SINAMICS S120 Commissioning Manual with Startdrive.

A.1.5.2 Requirements for communication

Check the communication settings using the following questions. If you answer "Yes" to the questions, you have correctly set the communication settings and can control the drive via the fieldbus.

- Is the drive correctly connected to the EtherNet/IP?
- Has a generic module been created in your control system?
- Have the bus interface and IP address been correctly set?
- Have the signals that the drive and the control system exchange been correctly interconnected?

A.1.5.3 Configuring EIP via the onboard PROFINET X150 interface

To communicate with a higher-level control via EIP, make the following settings for the PROFINET interface at the CU320-2 PN:

1. With p2030 = 10, set the firmware version of "EtherNet/IP".
2. Set the IP address using p8921.
   You can find the currently valid address in r8931.
3. Set the subnet mask using p8923.
   You can find the currently valid subnet mask in r8933.
4. Set the standard gateway using p8922.
   You can find the currently valid standard gateway in r8932.
5. Set the station name using p8920.
   You can find the currently valid station name in r8930.
6. Select the setting "Save and activate configuration" as interface configuration using p8925 = 2.
7. Save the data using command "Copy RAM to ROM".
   Then switch off the drive power supply.
8. Carry out a POWER ON (switch off the Control Unit and switch on again).
   Wait until all LEDs on the drive are dark before switching on. Your settings become active after switching on.

Result:

You have configured the onboard PROFINET X150 interface of the drive for communication via EIP .

A.1.5.4 Configuring EIP via the X1400 interface at the CBE20

To communicate with a higher-level control via EIP, make the following settings for the CBE20:

1. With p8835 = 4, set the firmware version of "EtherNet/IP".
2. Using p8941, set the IP address for the CBE20.
   You can find the currently valid address in r8951.
3. Set the subnet mask using p8943.
   You can find the currently valid subnet mask in r8953.
4. Set the standard gateway using p8942.
   You can find the currently valid standard gateway in r8952.
5. Set the station name using p8940.
   You can find the currently valid station name in r8950.
6. Select the setting "Save and activate configuration" as interface configuration using p8945 = 2.
7. Save the data using command "Copy RAM to ROM".
   Then switch off the drive power supply.
8. Carry out a POWER ON (switch off the Control Unit and switch on again).
   Wait until all LEDs on the drive are dark before switching on. Your settings become active after switching on.

Result:

You have configured interface X1400 of the CBE20 for communication via EIP .

A.1.5.5 Supported objects

Table A-35 Overview

Object class		Object name	Objects required	SINAMICS objects
hex	dec			
1 hex	1	Identity object (Page 207)	x	-
4 hex	4	Assembly Object (Page 207)	x	-
6 hex	6	Connection Management Object (Page 207)	x	-
32C hex	812	Siemens Drive Object (Page 207)	-	x
32D hex	813	Siemens Motor Data Object (Page 207)	-	x
F5 hex	245	TCP/IP Interface Object (Page 207)[1)]	x	-
F6 hex	246	Ethernet Link Object (Page 207)[1)]	x	-
300 hex	768	Stack Diagnostic Object	-	x
302 hex	770	Adapter Diagnostic Object	-	x
303 hex	771	Explicit Messages Diagnostic Object	-	x
304 hex	772	Explicit Message Diagnostic List Object	-	x

Object class		Object name	Objects required	SINAMICS objects
hex	dec			
401 hex	1025	Parameter object (Page 207)	-	x
402 hex ... 43E hex	1026...1086	Parameter object (Page 207)	-	x

1) These objects are part of the EtherNet/IP system management.

For Assembly Object "4 hex" you define the data length. Assembly Object is assigned a cycle in the control system.

Identity Object, Instance Number: 1 hex

Supported services

Class
- Get Attribute all
- Get Attribute single

Instance
- Get Attribute all
- Get Attribute single
- Reset

Table A-36 Class Attribute

No.	Service	Type	Name
1	get	UINT16	Revision
2	get	UINT16	Max Instance
3	get	UINT16	Num of Instances

Table A-37 Instance Attribute

No.	Service	Type	Name	Value/explanation
1	get	UINT16	Vendor ID	1251
2	get	UINT16	Device Type - Siemens Drive	 0C hex
3	get	UINT16	Product code	r0964[1]
4	get	UINT16	Revision	-
5	get	UINT16	Status	See the following table
6	get	UINT32	Serial number	Bit 0 ... 19: consecutive number; bits 20 ... 23: Production identifier bits 24 ... 27: Month of manufacture (0 = Jan, B = Dec) Bits 28 ... 31: Year of manufacture (0 = 2002)
7	get	Short String	Product name	max. length 32 byte

Table A-38 Explanation for No. 5 of the previous table

Byte	Bit	Name	Description
1	0	Owned	0: Converter is not assigned to a controller 1: Converter is assigned to a controller
	1	-	Reserved
	2	Configured	0: Ethernet/IP basic settings 1: Modified Ethernet/IP settings
	3	-	Reserved
	4 ... 7	Extended Device Status	0: Self-test or status not known 1: Firmware update active 2: At least one I/O connection with error 3: No I/O connections 4: Incorrect configuration in the ROM 5: Fatal fault 6: At least one I/O connection is active 7: All I/O connections in the quiescent state 8 ... 15: Reserved
2	8 ... 11	-	Not used
	12 ... 15	-	Reserved

Assembly Object, Instance Number: 4 hex

Supported services

Class
- Get Attribute single

Instance
- Get Attribute single
- Set Attribute single

Table A-39 Class Attribute

No.	Service	Type	Name
1	get	UINT16	Revision
2	get	UINT16	Max Instance
3	get	UINT16	Num of Instances

Table A-40 Instance Attribute

No.	Service	Type	Name	Value/explanation
3	get	Array of UINT8	Assembly	1 byte array

Connection Management Object, Instance Number: 6 hex

Supported services

Class
- Get Attribute all
- Get Attribute single

Instance
- Forward open
- Forward close
- Get Attribute single
- Set Attribute single

Table A-41 Class Attribute

No.	Service	Type	Name
1	get	UINT16	Revision
2	get	UINT16	Max Instance
3	get	UINT16	Num of Instances

Table A-42 Instance Attribute

No.	Service	Type	Name	Value/explanation
1	get	UINT16	OpenReqs	Counters
2	get	UINT16	OpenFormat Rejects	Counters
3	get	UINT16	OpenResource Rejects	Counters
4	get	UINT16	OpenOther Rejects	Counters
5	get	UINT16	CloseReqs	Counters
6	get	UINT16	CloseFormat Rejects	Counters
7	get	UINT16	CloseOther Rejects	Counters
8	get	UINT16	ConnTimeouts	Counters Number of bus errors

Siemens Drive Object, Instance Number: 32C hex

Supported services

Class
- Get Attribute single

Instance
- Get Attribute single
- Set Attribute single

Table A-43 Class Attribute

No.	Service	Type	Name
1	get	UINT16	Revision
2	get	UINT16	Max Instance
3	get	UINT16	Num of Instances

Table A-44 Instance Attribute

No.	Service	Name	Value/explanation
2	get, set	Commisioning state	p0010 Commissioning, parameter filter
3 ... 18	get	STW1	STW1 bit-by-bit access: Attr.3 = STW1.0 Attr.18 = STW1.15
19	get	Main setpoint	Main setpoint
20 ... 35	get	ZSW1	ZSW1 bit-by-bit access: Attr.20 = ZSW1.0 Attr.35 = ZSW1.15
36	get	Actual Frequency	Main actual value (actual frequency)
37	get, set	Ramp Up Time	p1120[0] ramp-function generator ramp-up time
38	get, set	Ramp Down Time	p1121[0] ramp-function generator ramp-down time
39	get, set	Current Limit	p0640[0] current limit
40	get, set	Frequency MAX Limit	p1082[0] maximum speed
41	get, set	Frequency MIN Limit	p1080[0] minimum speed
42	get, set	OFF3 Ramp Down Time	p1135[0] OFF3 ramp-down time
43	get, set	PID Enable	p2200[0] technology controller enable
44	get, set	PID Filter Time Constant	p2265 Technology controller actual value filter time constant
45	get, set	PID D Gain	p2274 technology controller differentiation time constant
46	get, set	PID P Gain	p2280 Technology controller proportional gain
47	get, set	PID I Gain	P2285 Technology controller integral action time
48	get, set	PID Up Limit	p2291 technology controller maximum limiting
49	get, set	PID Down Limit	p2292 technology controller minimum limiting
50	get	Speed setpoint	r0020 speed setpoint
51	get	Output Frequency	r0024 output frequency
52	get	Output Voltage	r0025 output voltage
53	get	DC Link Voltage	r0026[0] DC link voltage
54	get	Actual Current	r0027 current actual value
55	get	Actual Torque	r0031 torque actual value
56	get	Output power	r0032 actual active power value
57	get	Motor Temperature	r0035[0] motor temperature
58	get	Power Unit Temperature	r0037[0] power unit temperature
59	get	Energy kWh	r0039 energy indicator
60	get	CDS Eff (Local Mode)	r0050 active command data set
61	get	Status Word 2	r2089[1] status word 2
62	get	Control Word 1	r0898 control word 1
63	get	Motor Speed (Encoder)	r0061 speed actual value

No.	Service	Name	Value/explanation
64	get	Digital Inputs	r0722 digital inputs status
65	get	Digital Outputs	r0747 digital outputs status
66	get	Analog Input 1	r0752[0] analog input 1
67	get	Analog Input 2	r0752[1] analog input 2
68	get	Analog Output 1	r0774[0] analog output 1
69	get	Analog Output 2	r0774[1] analog output 2
70	get	Fault Code 1	r0947[0] fault number 1
71	get	Fault Code 2	r0947[1] fault number 2
72	get	Fault Code 3	r0947[2] fault number 3
73	get	Fault Code 4	r0947[3] fault number 4
74	get	Fault Code 5	r0947[4] fault number 5
75	get	Fault Code 6	r0947[5] fault number 6
76	get	Fault Code 7	r0947[6] fault number 7
77	get	Fault Code 8	r0947[7] fault number 8
78	get	Pulse Frequency	r1801 actual pulse frequency
79	get	Alarm Code 1	r2110[0] alarm number 1
80	get	Alarm Code 2	r2110[1] alarm number 2
81	get	Alarm Code 3	r2110[2] alarm number 3
82	get	Alarm Code 4	r2110[3] alarm number 4
83	get	PID setpoint Output	r2260 technology controller setpoint after the ramp-function generator
84	get	PID Feedback	r2266 technology controller actual value after the filter
85	get	PID Output	r2294 technology controller output signal

The instances are assigned using the slot sequence in p0978.

Siemens Motor Data Object, Instance Number: 32D hex

Supported services

Class
- Get Attribute single

Instance
- Get Attribute single
- Set Attribute single

Object "32D hex" is only available on "SERVO" and "VECTOR" drive objects:

- SERVO DO = 11
- VECTOR DO = 12

Table A-45 Class Attribute

No.	Service	Type	Name
1	get	UINT16	Revision
2	get	UINT16	Max Instance
3	get	UINT16	Num of Instances

Table A-46 Instance Attribute

No.	Service	Type	Name	Value/explanation
2	get, set	UINT16	Commisioning state	p0010 commissioning parameter filter
3	get, set	INT16	Motor Type	p0300 motor type
6	get, set	REAL	Rated Current	p0305 rated motor current
7	get, set	REAL	Rated Voltage	p0304 rated motor voltage
8	get, set	REAL	Rated Power	p0307 rated motor power
9	get, set	REAL	Rated Frequency	p0310 rated motor frequency
10	get, set	REAL	Rated Temperature	p0605 threshold and temperature value for monitoring the motor temperature
11	get, set	REAL	Max Speed	p0322 maximum motor speed
12	get, set	UINT16	Pole pair number	p0314 motor pole pair number
13	get, set	REAL	Torque Constant	p0316 motor torque constant
14	get, set	REAL	Inertia	p0341 motor moment of inertia
15	get, set	REAL	Base Speed	p0311 rated motor speed
19	get, set	REAL	Cos Phi	p0308 rated motor power factor

The instances are assigned using the slot sequence in p0978.

Supported services

Class
- Get Attribute all
- Get Attribute single

Instance
- Get Attribute all
- Get Attribute single
- Set Attribute single

Table A-47 Class Attribute

No.	Service	Type	Name
1	get	UINT16	Revision
2	get	UINT16	Max Instance
3	get	UINT16	Num of Instances

Table A-48 Instance Attribute

No.	Service	Type	Name	Value/explanation
1	get	UNIT32	Status	Fixed value: 1 hex 1: Configuration acknowledged, by DHCP or saved values
2	get	UNIT32	Configuration Capability	Fixed value: 94 hex 4 hex: DHCP supported, 10 hex: Configuration can be adjusted, 80 hex: ACD-capable
3	get, set	UNIT32	Configuration Control	1 hex: Saved values 3 hex: DHCP

No.	Service	Type	Name	Value/explanation
4	get	UNIT16	Physical Link	Path Size (in WORDs); fixed value: 2 hex
		UNIT8		Path (20 hex, F6 hex, 24 hex, 05 hex, where 5 hex is the number of instances of F6 hex): 4 physical ports plus an internal port).
5	get, set	STRING	Interface Configuration	r61000 Name of Station
		UNIT32		r61001 IP address
6	get, set	UNIT16	Host Name	Host Name Length
		STRING		-
10	get, set	UNIT8	Select ACD	local OM flash: 0: Disabled, 1: Enabled
11	get, set	UNIT8	Last Conflict Detected	local OM flash ACD Activity
		UNIT8		local OM flash Remote MAC
		UNIT8		local OM flash ARP PDU

Link Object, Instance Number: F6 hex

Supported services

Class
- Get Attribute all
- Get Attribute single

Instance
- Get Attribute all
- Get Attribute single
- Set Attribute single

Table A-49 Class Attribute

No.	Service	Type	Name
1	get	UINT16	Revision
2	get	UINT16	Max Instance
3	get	UINT16	Num of Instances

Table A-50 Instance Attribute

No.	Service	Type	Name	Value/explanation
1	get	UINT32	Interface Speed	0: link down, 10: 10 Mbps, 100: 100 Mbps
2	get	-	Interface Flags	Bit 1: Link-Status Bit 2: Duplex Mode (0: half duplex, 1 duplex) Bit 3 - 5: Automatic state identification Bit 6: Reset required Bit 7: Local hardware fault (0 = ok)
3	get	ARRAY	Physical Address	r8935 Ethernet MAC address

No.	Service	Type	Name	Value/explanation
4	get, get_and_clear	Struct of	Interface Counters	Optional, required if the "Media Counters Attribute" is implemented.
		UINT32	In Octets	Received octets
		UINT32	In Ucast Packets	Received Unicast packets
		UINT32	In NUcast Packets	Received non-Unicast packets
		UINT32	In Discards	Incoming packets, not processed
		UINT32	In Errors	Incoming packets with errors
		UINT32	In Unknown Protos	Incoming packets with unknown protocol
		UINT32	Out Octets	Sent octets
		UINT32	Out Ucast Packets	Sent Unicast packets
		UINT32	Out NUcast packets	Sent non-Unicast packets
		UINT32	Out Discards	Outgoing packets, not processed
		UINT32	Out Errors	Outgoing packets, with errors
5	get, get_and_clear	Struct of	Media Counters	Media-specific counters
		UINT32	Alignment Errors	Structure received, which does not match the number of octets
		UINT32	FCS Errors	Structure received, which does not pass the FCS check
		UINT32	Single Collisions	Structure successfully transmitted, precisely one collision
		UINT32	Multiple Collisions	Structure successfully transmitted, several collisions
		UINT32	SQE Test Errors	Number of SQE errors
		UINT32	Deferred Transmissions	First transmission attempt delayed
		UINT32	Late Collisions	Number of collisions that occurred delayed by 512 bit timers to the request
		UINT32	Excessive Collisions	Transmission unsuccessful as a result of intensive collisions
		UINT32	MAC Transmit Errors	Transmission unsuccessful as a result of an internal MAC sublayer transmission error.
		UINT32	Carrier Sense Errors	Number of errors when attempting to send a request frame, where the transmission condition was lost or was not assigned
		UINT32	Frame Too Long	Structure too large
		UINT32	MAC Receive Errors	Transmission unsuccessful as a result of an internal MAC sublayer receive error.
6	get, set	Struct of	Interface Control	-
		UINT16	Control Bits	-
		UINT16	Forced Interface Speed	-

No.	Service	Type	Name	Value/explanation
10	get	String	Interface_Label	Interface-Label
11	get	-	Interface Capability	Bit 0: Manual Setting Bit 1: Auto-negotiate Bit 2: Auto-MDIX Bit 3: Manual Speed/Duplex Bit 4 - 31: reserved Remaining: Speed/Duplex Options

Parameter Object, Instance Number: 401 hex

Supported services

Class
- Get Attribute all

Instance
- Get Attribute all
- Set Attribute single

Table A-51 Class Attribute

No.	Service	Type	Name
1	get	UINT16	Revision
2	get	UINT16	Max Instance
3	get	UINT16	Num of Instances

Parameter access to drive object 0 (DO 0) is realized via this class.

Example: Read parameter 2050[10] (connector output to interconnect the PZD received from the fieldbus controller)

Get Attribute single function with the following values:

- Class = 401 hex
- Instance = 2050 = 802 hex ≙ parameter number
- Attribute = 10 = A hex ≙ Index 10

Example: Parameter 1520[0] writing (upper torque limit)

Set Attribute single function with the following values:

- Class = 401 hex
- Instance = 1520 = 5F0 hex ≙ parameter number
- Attribute = 0 = 0 hex ≙ index 0
- Data = 500.0 (value)

Parameter Object, Instance Number: 401 hex ... 43E hex

Supported services

Class
- Get Attribute All
- Get Attribute Single

Instance
- Get Attribute Single
- Set Attribute Single

Table A-52 Class Attribute

No.	Service	Type	Name
1	get	UINT16	-
2	get	UINT16	Max slot num
3	get	UINT16	Max slot ID

Parameter access to drive object 0 (DO 0) is realized via this class.

The class structure is analog to 401 hex. Drive object (DO) is selected via the class number.

Example:

0x401 -> DO 1

0x402 -> DO 2

...

0x43E -> DO 62

A.1.5.6 Integrating the drive device into the EIP network via DHCP

Integrating the drive via the PROFINET onboard interface X150 into the EIP network

Proceed as follows to integrate the drive into the EIP network:

1. Set p8924 (PN DHCP mode) = 2 or 3

Parameterization	Meaning
p8924 = 2	The DHCP server assigns the IP address based on the MAC address.
p8924 = 3	The DHCP server assigns the IP address based on the station name.

2. Save the settings with p8925 = 2.
   The next time that it is run-up, the drive retrieves the IP address made available by a DHCP server. After the drive has run-up, you can address the drive as Ethernet participant.

Note

Immediate switchover without restart

The switchover to DHCP is performed immediately and without a restart if the change is carried out with the EIP command "Set Attribute Single" (class F5 hex, attribute 3), e.g. using:

- An EIP control
- An EIP commissioning tool

Result:

You have integrated the drive into the EIP network via DHCP.

Displays

- r8930: Station name of the onboard PROFINET interface X150
- r8934: DHCP mode of the onboard PROFINET interface X150
- r8935: MAC address of the onboard PROFINET interface X150

Integrating the drive into the EIP network via the X1400 interface at the CBE20

Integrating the drive into the EIP network via interface X1400 at the CBE20

1. Set p8944 (CBE2x DHCP mode) = 2 or 3.

Parameterization	Meaning
p8944 = 2	The DHCP server assigns the IP address based on the MAC address.
p8944 = 3	The DHCP server assigns the IP address based on the station name.

2. Save the settings with p8945 = 2.
   The next time that it is run-up, the drive retrieves the IP address made available by a DHCP server. After the drive has run-up, you can address the drive as Ethernet participant.

Note

Immediate switchover without restart

The switchover to DHCP is performed immediately and without a restart if the change is carried out with the EIP command "Set Attribute Single" (class F5 hex, attribute 3), e.g. using:

- An EIP control
- An EIP commissioning tool

Result:

You have integrated the drive into the EIP network via DHCP.

Displays

- r8950: Station name of interface X1400 at the CBE20
- r8954: DHCP mode of interface X1400 at the CBE20
- r8955: MAC address of interface X1400 at the CBE20

A.1.5.7 Messages and parameters

Faults and alarms (see SINAMICS S120/S150 List Manual)

- F08501 (N,A) PN/COMM BOARD: Setpoint timeout
- F01910 (N,A) Fieldbus: Setpoint timeout
- A08526 (F) PN/COMM BOARD: No cyclic connection
- A01980 (F) PN: Cyclic connection interrupted
- A50011 (F) EtherNetIP/COMM BOARD: Configuration error
- A01906 (F) EtherNet/IP Configuration error

Overview of important parameters (see SINAMICS S120/S150 List Manual)

- p0978[0...n] List of drive objects
- p0922 IF1 PROFIdrive PZD telegram selection
- p0999[0...99] List of modified parameters 10
- p2030 Fieldbus interface protocol selection
- p8835 CBE20 firmware selection
- p8842 COMM BOARD activate send configuration
- p8920[0...239] PN name of station
- p8921[0...3] PN IP address
- p8922[0...3] PN default gateway
- p8923[0...3] PN Subnet Mask
- p8924 PN DHCP mode
- p8925 Activate PN interfaces configuration
- p8930[0...239] PN Name of Station actual
- p8931[0...3] PN IP Address actual
- p8932[0...3] PN Default Gateway actual
- p8933[0...3] PN Subnet Mask actual
- p8934 PN DHCP Mode actual
- p8935[0...5] PN MAC Address
- p8940[0...239] CBE2x Name of Station
- p8941[0...3] CBE2x IP address
- p8942[0...3] CBE2x Default Gateway
- p8943[0...3] CBE2x Subnet Mask
- p8944 CBE2x DHCP mode
- p8945 CBE2x interfaces configuration
- r8950[0...239] CBE2x Name of Station actual
- r8951[0...3] CBE2x IP address actual
- r8952[0...3] CBE2x Default Gateway actual
- r8953[0...3] CBE2x Subnet Mask actual

- r8954 CBE2x DHCP Mode actual
- r8955[0...5] CBE2x MAC address

A.1.6 Communication via SINAMICS Link

A.1.6.1 Basic principles of SINAMICS Link

A drive unit (with a node number) most frequently comprises a Control Unit with a number of connected drive objects (DOs). SINAMICS Link allows data to be directly exchanged between up to 64 CU320-2 PN or CU320-2 DP Control Units or CUD. All of the participating Control Units must be equipped with a CBE20 in order that SINAMICS Link functions. Possible applications are, for example:

- Torque distribution for n drives
- Setpoint cascading for n drives
- Load distribution of drives coupled through a material web
- Master/slave function for infeed units
- Links between SINAMICS DC-MASTER and SINAMICS S120

Requirements

The following preconditions must be fulfilled to operate SINAMICS Link:

- One CBE20 must be inserted for each drive object.
- In the isochronous mode (p8812[0] = 1), the bus cycle time (p8812[1]) must be an integer multiple of p0115[0] (current controller sampling time).
- In the isochronous mode, the current controller sampling time must be set to 125 µs, 250 µs or 500 µs. A sampling time with 400 µs is not permitted. For 400 µs, alarm A01902[4] is output. As countermeasure, set the current controller sampling time with p0115[0] to 500 µs.

Note

The "SINAMICS Link" function is not available for the Control Unit CU310-2.

Note

SINAMICS Link for chassis format

For the following devices in the chassis format, you must set parameter p0115[0] to 250 µs or 500 µs:

- 380 - 480 V 3-phase AC: All devices with rated current index ≥ 605 A
- 500 - 690 V 3-phase AC: All devices

Send and receive data

The SINAMICS Link telegram contains 32 indices (0...31) for the process data (PZD1...32). Each PZD is precisely 1 word long (= 16 bits). Indices that are not required are automatically filled with "0". There is always a fixed assignment between the index and PZD: The index i corresponds to PZD i+1.

Index	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
PZD	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

SINAMICS Link telegram content, Part 1

Index	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
PZD	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

SINAMICS Link telegram content, Part 2

Each transfer cycle, every SINAMICS Link node can send 1 telegram with 32 PZD. Each node receives all of the telegrams that are sent. For each transfer cycle clock, a node can select and process up to 32 PZD from all telegrams that have been received. The converter can send and receive single words and double words. You must write double words in two consecutive PZDs.

Limitations:

- Within a telegram, a PZD may only be sent and received once. If a PZD occurs more than once in a telegram, then Alarm A50002 or A50003 is output.
- It is not possible to read in your own send data. SINAMICS S then initiates the corresponding alarms. The following alarms are possible:
  - A50006: According to what has been parameterized, data sent by itself should be received. This action is not permitted.
  - A50007: The send telegram word is larger than possible in the project.
  - A50008: The receive telegram word is larger than possible in the project.
- The maximum number of PZDs that can be received and sent also depends on the drive object. The number of PZDs that can be evaluated corresponds to communication according to PROFIdrive; however, for SINAMICS Link, it is limited to a maximum of 32 PZDs.
- If CBE20 parameters were changed as a result of a project download, then alarm A08531 is output. In this case, a POWER ON is required to activate the values.

Transmission time

With SINAMICS Link, a transmission time of up to 500 µs is possible (with a max. controller cycle of 500 µs; synchronous bus cycle of 500 µs).

Bus cycle and number of nodes

You can operate the bus cycle of the SINAMICS Link with the current controller cycle, either synchronized or non-synchronized.

- You set synchronized operation with p8812[0] = 1. A maximum of 64 nodes can then communicate with one another via SINAMICS Link. To do so, set the maximum number of nodes with p8811 (project selection):

Number of nodes/ project no.	PZD count	Bus cycle (ms)
64	16	1 or 2
16	16	0.5
12	24	0.5
8	32	0.5

- A maximum of 64 participants can communicate with one another via SINAMICS Link.

If you change at least one of the parameters p8811, p8812, p8835 or p8836, then you must carry out a POWER ON to accept the settings.

A.1.6.2 Configuring and commissioning

When commissioning, proceed as follows:

1. Set the Control Unit parameter p0009 = 1 (device configuration).
2. Set the Control Unit parameter p8835 = 3 (SINAMICS Link).
3. Using p8839, define which interface should be used (for example for IF1: p8839[0] = 2).
4. If SINAMICS Link is assigned to IF1, set parameter p2037 of the drive objects to 2 (do not freeze setpoints).
   If SINAMICS Link was assigned IF2, then p8837 must be used for the setting.
5. Assign the nodes in parameter p8836 to the SINAMICS Link node number.
   The first Control Unit is always assigned the number 1. Node number 0 means that for this Control Unit SINAMICS Link has been shut down. Observe the specifications under "Topology".
6. Check and/or correct the following parameters:
   – p8811 must be identical for all nodes
   – p8812[1] must be identical for all nodes
   – p8812[0] may be different for local nodes
7. Set the Control Unit parameter p0009 = 0 (ready).
8. Execute a "Copy RAM to ROM".
9. Carry out a POWER ON (switch off the Control Unit and switch on again).

Sending data

Note

The parameters listed in the following description refer to the assignment of SINAMICS Link to IF1. If you assigned SINAMICS Link to IF2, then you find the corresponding parameters in the "Table A-57 Corresponding parameters (Page 228)".

In this example, the first "Control Unit 1" node has two drive objects: "Drive 1" and "Drive 2". Proceed as follows to send data:

1. If SINAMICS Link is assigned to IF1, then for each drive object, in its associated parameter p2051[0...31], you define which data (PZDs) should be sent.
   If SINAMICS Link was assigned IF2, then p8851 must be used for the setting. The data is simultaneously reserved in the send slot of the p8871[0...31].
2. Enter the double words in p2061[x].
   Double word data is simultaneously written to p8861[0...31].
3. For each drive object, allocate the send parameters in p8871[0...31] to a send slot of its own node.

Table A-53 Compile send data of drive 1 (DO2)

p2051[x] Index	p2061[x] Index	Contents	From parameter	Telegram word p8871
0	-	ZSW1	r0899	1
-	1	Actual speed value part 1	r0061[0]	2
-		Actual speed value part 2		3
-	3	Actual torque value part 1	r0080	4
-		Actual torque value part 2		5
5	-	Actual fault code	r2131	6
6	-	0	0	0
...	-	...	-	...
15	-	0	0	0
...	-	...	-	...
31	-	0	0	0

Table A-54 Compile send data of drive 2 (DO3)

p2051[x] Index	p2061[x] Index	Contents	From parameter	Slots in the send buffer p8871[x]	
				x	Telegram word
-	-	-	-	0...5[1)]	0
0	-	ZSW1	r0899	6	7
-	1	Actual speed value part 1	r0061[0]	7	8
-		Actual speed value part 2		8	9

p2051[x] Index	p2061[x] Index	Contents	From parameter	Slots in the send buffer p8871[x]	
				x	Telegram word
-	3	Actual torque value part 1	r0080	9	10
-		Actual torque value part 2		10	11
5	-	Actual fault code	r2131	11	12
6	-	0	0	12	0
...		...		...	...
15	-	0	0	15	0
...	-	...	-	...	...
31	-	0	0	31	0

[1] 0...5 here remain free, as they are already assigned by DO2.

Table A-55 Compile send data of Control Unit 1 (DO1)

p2051[x] Index	p2061[x] Index	Contents	From parameter	Slots in the send buffer p8871[x]	
				x	Telegram word
-	-	-	-	0...11[2]	0
0	-	Control word, faults/alarms	r2138	12	13
-	1	Missing enables part 1	r0046	13	14
-		Missing enables part 2		14	15
15	-	0	0	15	0
...	-	...	-	...	...
31	-	0	0	31	0

[2] 0...11 here remain free, as they are already assigned by DO2 and DO3.

Send slots PZD 16 to 31 are not required for this telegram and are therefore filled with a zero.

1. For double words (e.g. 1 + 2), assign two consecutive send slots, e.g. p2061[1] => p8871[1] = PZD 2 and p8871[2] = PZD 3.
2. Enter the following PZD into the next parameter slots of p2051[x] or p2061[2x].
3. Populate the unused slots of p8871[0...31] with zeros.
4. The sequence of the PZDs in the send telegram of this node are defined in parameter p8871[0...31] by the entries in the required slots.

Receiving data

The sent telegrams of all nodes are simultaneously available at the SINAMICS Link. Each telegram has a length of 32 PZD. Each telegram has a marker of the sender. You select those PZD that you want to receive for the relevant node from all telegrams. You can process a maximum of 32 PZD.

Note

If you have not deactivated the evaluation of bit 10 with p2037 = 2, the first word of the receive data (PZD 1) must be a control word, where bit 10 = 1 is set.

In this example, Control Unit 2 receives selected data from the telegram of Control Unit 1. Proceed as follows to receive data:

1. In parameter p8872[0...31] enter the address of the node for which you want to read one or more PZDs (e.g. p8872[3] = 1 → from node 1, read in PZD 4, p8872[15] = 0 → do not read in PZD 16).
2. After setting the parameters, using parameter r2050[0...31] or r2060[0...31] you can read out the values.

Table A-56 Receive data for Control Unit 2

From the sender		Receiver					
Transfer from	Tel. word[1] p8871[x]	Address p8872[x]	Receive buffer p8870[x]	Data transferred in		Parameter	Contents
				r2050[x]	r2060[x]		
p2051[0]	0	1	PZD 1	0	-	r0899	ZSW1
p2061[1]	1	1	PZD 2	-	1	r0061[0]	Actual speed value part 1
	2	1	PZD 3	-		r0061[0]	Actual speed value part 2
p2061[3]	3	1	PZD 4	-	3	r0080	Actual torque value part 1
	4	1	PZD 5	-			Actual torque value part 2
p2051[5]	5	1	PZD 6	5	-	r2131	Actual fault code
p2051[4]	6	1	PZD 7	6	-	r0899	ZSW1
p2061[5]	7	1	PZD 8	-	7	r0061[0]	Actual speed value part 1
	8	1	PZD 9	-			Actual speed value part 2
p2061[6]	9	1	PZD 10	-	9	r0080	Actual torque value part 1
	10	1	PZD 11	-			Actual torque value part 2
p2051[7]	11	1	PZD 12	11	-	r2131	Actual fault code
p2051[8]	12	1	PZD 13	12	-	r2138	Control word, faults/alarms
p2061[9]	13	1	PZD 14	-	13	r0046	Missing enables part 1
	14	1	PZD 15	-			Missing enables part 2
-	15	0	PZD 16	15	-	0	Empty
...	...	...	...	...	...	...	...
-	31	0	PZD 32	31	0	0	-

[1] Tel.word = telegram word

Note

For double words, two PZD must be read in succession. To do this, read in a 32 bit setpoint, which is on PZD 2 + PZD 3 of the telegram of node 2. Emulate this setpoint on PZD 2 + PZD 3 of node 1: p8872[1] = 2, p8870[1] = 2, p8872[2] = 2, p8870[2] = 3

Activating the SINAMICS Link

To activate SINAMICS Link connections, perform a POWER ON for all nodes.

Without POWER ON, the following can be changed:

- The assignments of p2051[x]/2061[2x] and the links of the read parameters r2050[x]/2060[2x]
- Parameters p8870, p8871, and p8872 In this case, the SINAMICS Link connections can also be connected via p8842 = 1.

A.1.6.3 Topology

Only a line topology with the following structure is permitted for SINAMICS Link. You must manually set the parameters in the parameter views of the Control Units and drive objects. To do this, use the Startdrive commissioning tool.

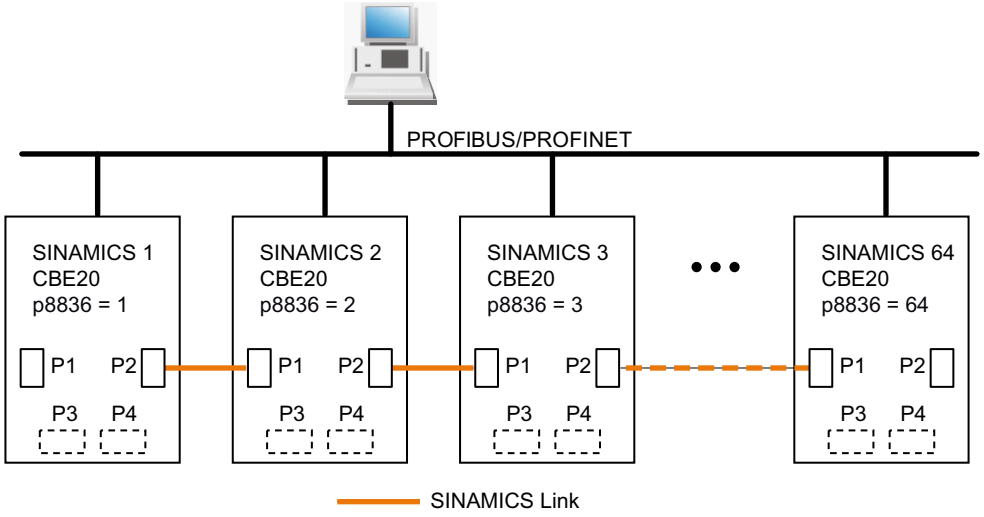


Figure A-51 Maximum topology

Features

- The CBE20 can be assigned to IF1 or IF2 when SINAMICS Link is used.
  The interface, assigned to the CBE20, must be switched into synchronous operation if p8812[0] = 1 is set.
  You must also make the following parameter settings in order to assign, e.g. IF1 to SINAMICS Link:
  - For IF1: p8839[0] = 2 (COMM BOARD)
  - For IF2: p8839[1] = 1 (Control Unit onboard)

  The data in the additional description are applicable for the case (IF1 ≙ SINAMICS Link).
- The number of the respective node must be entered manually in parameter p8836. Each node must be assigned a different number. Enter the numbers in ascending order starting with 1.
- If p8836 is set to 0, the nodes and the complete following line is shut down for SINAMICS Link.
- Gaps in the numbering are not permitted, as then SINAMICS Link would not function.
- The node with the number 1 is automatically the sync master of the communication link.
- The ports of the CBE20 must be interconnected strictly in accordance with the above diagram. You must always connect port 2 (P2) of node n with port 1 (P1) of node n + 1.
- In the "SINAMICS Link" mode, ports 3 and 4 of the CBE20 can only be used in conjunction with the Startdrive commissioning tool.

Corresponding parameters for IF1 or IF2

Use different parameters for configuring, depending on which interface SINAMICS Link is assigned:

Table A-57 Corresponding parameters

Parameters	IF1	IF2
Setting of the processing mode for PROFIdrive STW1.10 "Control by PLC".	p2037	p8837
Connector output to interconnect the PZD (setpoints) received from the fieldbus controller in the word format.	r2050	r8850
Selects the PZD (actual values) to be sent to the fieldbus controller in the word format.	p2051	p8851
Displays the PZD (actual values) sent to the fieldbus controller in the word format.	r2053	r8853
Connector output to interconnect the PZD (setpoints) received from the fieldbus controller in the double word format.	r2060	r8860
Selects the PZD (actual values) to be sent to the fieldbus controller in the double word format.	p2061	p8861
Displays the PZD (actual values) sent to the fieldbus controller in the double word format.	r2063	r8863

A.1.6.4 Examples: Transmission times for SINAMICS Link

Example 1: Transmission times at a communication cycle of 1 ms

p2048 or p8848 = 1 ms

Bus cycle	Transmission time			
	Sync both	Sync send	Sync receive	Async both
0.5	1.0	1.5	1.3	1.6
1.0	1.5	2.1	2.1	2.2
2.0	3.0	3.6	3.1	2.8

Example 2: Transmission times at a communication cycle of 4 ms

p2048 or p8848 = 4 ms

Bus cycle	Transmission time			
	Sync both	Sync send	Sync receive	Async both
0.5	1.0	3.0	2.8	4.6
1.0	1.5	3.6	3.6	5.2
2.0	3.0	5.1	4.6	5.8

A.1.6.5 Communication failure when booting or in cyclic operation

If at least one sender does not correctly boot after commissioning or fails in cyclic operation, then alarm A50005 is output to the other nodes: "Sender was not found on the SINAMICS Link." The message contains the number of the faulted node. After you have resolved the fault at the node involved and the system has identified the node, the system automatically withdraws the alarm.

If several nodes are involved, the message occurs a multiple number of times consecutively with different node numbers. After you have resolved all of the faults, the system automatically withdraws the alarm.

When a node fails in cyclic operation, in addition to alarm A50005, fault F08501 is output: "COMM BOARD: Monitoring time, process data expired"

At node 1, fault F08501 is not triggered. This node should be used for specifying setpoint values to other nodes.

A.1.6.6 Example

Task

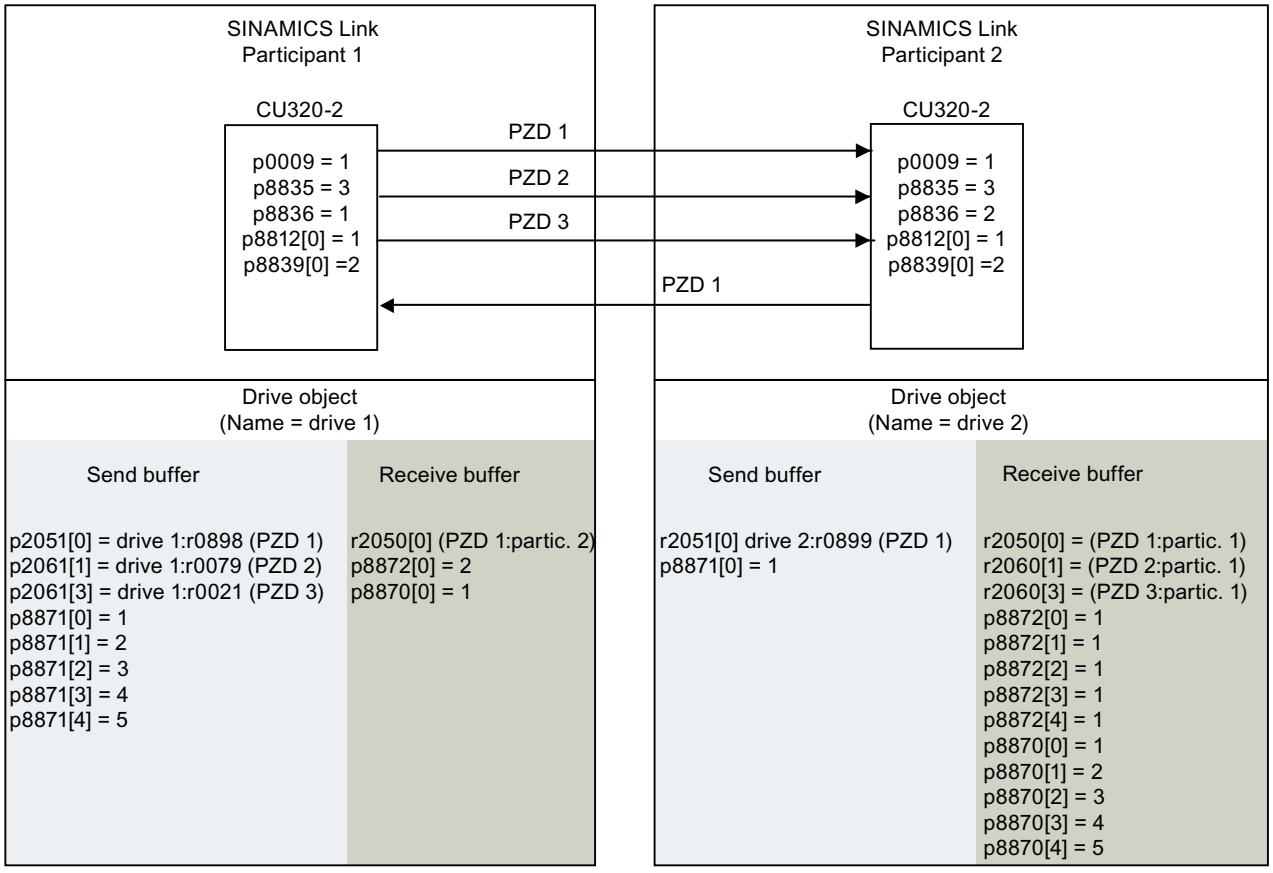
Configure SINAMICS Link for two nodes and transfer the following values:

- Send data from node 1 to node 2
  - r0898 CO/BO: Control word, sequence control, drive 1 (1 PZD), in the example PZD 1
  - r0079 CO: Total torque setpoint (2 PZD), in the example PZD 2
  - r0021 CO: Smoothed actual speed (2 PZD), in the example PZD 3
- Send data from node 2 to node 1
  - r0899 CO/BO: Status word, sequence control, drive 2 (1 PZD), in the example PZD 1
- IF1 is used for SINAMICS Link.

Procedure

1. For all nodes, set p0009 = 1 to change the device configuration.
2. For all CBE20 nodes, set the "SINAMICS Link" mode using p8835 = 3.
3. Limit the maximum number of nodes for all nodes with p8811 = 8. By setting p8811, parameter p8812[1] is preassigned, and parameter p8836, if necessary, is corrected.
4. Assign the node numbers for the devices involved:
   - Node 1 (≙ device 1): p8836 = 1
   - Node 2 (≙ device 2): p8836 = 2
5. Set all CBE20 to the isochronous mode by setting p8812[0] = 1.
6. Make the following interface setting for all nodes:
   - For IF1: p8839[0] = 2 (COMM BOARD)
   - For IF2: p8839[1] = 1 (Control Unit onboard)
7. For both nodes p0009 = 0, carry out a "Copy RAM to ROM" followed by a POWER ON in order to activate the modified firmware versions and the new settings in the CBE20.
8. Define the send data for node 1:
   - Define the PZD that node 1 should send:
     p2051[0] = drive 1:r0898 (PZD 1)
     p2061[1] = drive1:r0079 (PZD 2 + PZD 3)
     p2061[3] = drive1:r0021 (PZD 4 + PZD 5)
   - Place these PZD in the send buffer (p8871) of node 1:
     p8871[0] = 1 (r0898)
     p8871[1] = 2 (r0079 1st part)
     p8871[2] = 3 (r0079 2nd part)
     p8871[3] = 4 (r0021 1st part)
     p8871[4] = 5 (r0021 2nd part)

9. Define the receive data for node 2:
   - Specify that the data placed in the receive buffer p8872 of node 2 in locations 0 to 4 will be received by node 1:
     p8872[0] = 1
     p8872[1] = 1
     p8872[2] = 1
     p8872[3] = 1
     p8872[4] = 1
   - Specify that PZD1, PZD2, and PZD3 of node 1 will be placed in the receive buffer p8870 of node 2 in locations 0 to 4:
     p8870[0] = 1 (PZD1)
     p8870[1] = 2 (PZD2 1st part)
     p8870[2] = 3 (PZD2 2nd part)
     p8870[3] = 4 (PZD3 1st part)
     p8870[4] = 5 (PZD3 2nd part)
   - r2050[0], r2060[1] and r2060[3] subsequently contain (after step 13) the values of PZD 1, PZD 2 and PZD 3 of node 1.
10. Define the send data for node 2:
    - Specify the PZD that node 2 should send:
      :p2051[0] = drive1:r0899 (PZD length is 1 word)
    - Place this PZD in the send buffer (p8871) of node 2:
      p8871[0] = 1
11. Define the receive data for node 1:
    - Specify the data that should be placed in the receive buffer p8872 of node 1 in location 0, received from node 2:
      p8872[0] = 2
    - Define that PZD1 of node 2 is saved in the receive buffer p8870 of node 1 in location 0:
      p8870 [0] = 1
    - r2050[0] subsequently contains (after step 13) the value of PZD 1 of node 2.
12. At the two nodes carry-out a "Copy RAM to ROM" to backup the parameterization and the data.
13. Set p8842 =1, to activate parameters p8870, p8871 and p8872.



r0021: Speed actual value smoothed
r0079: Total torque setpoint
r0898: Control word sequence control drive 1
r0899: Status word sequence control drive 2

Figure A-52 SINAMICS Link: Configuration example

A.1.6.7 Function diagrams and parameters

Function diagrams (see SINAMICS S120/S150 List Manual)

- 2197 Control Unit communication - SINAMICS Link overview (r0108.31 = 1, p8835 = 3)
- 2198 Control Unit communication - SINAMICS Link configuration (r0108.31 = 1, p8835 = 3)
- 2199 Control Unit communication - SINAMICS Link receive data (r0108.31 = 1, p8835 = 3)
- 2200 Control Unit communication - SINAMICS Link send data (r0108.31 = 1, p8835 = 3)

Overview of important parameters (see SINAMICS S120/S150 List Manual)

- p0115[0] Current controller sampling time
- p2037 IF1 PROFIdrive STW1.10 = 0 mode
- r2050[0...31] CO: IF1 PROFIdrive PZD receive word
- p2051[0...31] CI: IF1 PROFIdrive PZD send word
- r2060[0...30] CO: IF1 PROFIdrive PZD receive double word
- p2061[0...30] CI: IF1 PROFIdrive PZD send double word
- p8811 SINAMICS Link project selection
- p8812[0...1] SINAMICS Link cycle settings
- p8835 CBE20 firmware selection
- p8836 SINAMICS Link node address
- p8839[0...1] PZD interface hardware assignment
- p8870[0...31] SINAMICS Link PZD receive word
- p8871[0...31] SINAMICS Link PZD send word
- p8872[0...31] SINAMICS Link PZD receive address

A.1.7 Communication via USS

The USS protocol is a serial data link between a master and up to 31 slaves.

A master is, for example:

- A programmable logic controller (e.g. SIMATIC S7-200)
- A PC

The converter is always a slave.

The maximum cable length is:

Maximum cable length	Baud rate	Maximum number of nodes
1200 m	≤ 38400 bit/s	32
1000 m	187500 bit/s	30

Interface for the USS protocol

The X140 serial interface is located on the underside of the Control Unit.

A.1.7.1 Basic settings for communication

Procedure

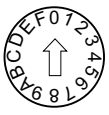
Proceed as follows to set communication via USS for CU320-2 DP or CU310-2 DP:

1. Set the bus protocol via p2030:
   p2030 = 6
2. Set the converter address.
3. Make additional changes based on the parameters listed in the following section.
4. Back up the settings so that they are protected against power failure.

Setting the address

Set the address as a hexadecimal value via 2 rotary coding switches. You can set values from 0_{dec} (00_{hex}) to 127_{dec} ($7F_{hex}$). At the upper rotary coding switch (H) you set the hexadecimal value for 16^1 and at the lower rotary coding switch (L) you set the hexadecimal value for 16^0.

Table A-58 Address switches

Rotary coding switches	Significance	Examples	
		21_{dec}	**31_{dec}**
		15_{hex}	**$1E_{hex}$**
 USS H	$16^1 = 16$	1	2
 USS L	$16^0 = 1$	5	3

Setting the address

Observe the properties of the rotary coding switch:

- The rotary coding switches used to set the address are located beneath the cover.
- The factory setting for the rotary coding switches is 0_{dec} (00_{hex}).
- The currently set address of the rotary coding switch is displayed in parameter r2057.
- When several Control Units are connected to a USS communication, you set the addresses with a value different to the factory setting. Each address can only be assigned once. Either set the address in absolute terms using the rotary coding switches or selectively in parameter p2021. Each change made to the bus address is not effective until POWER ON.

Note

- Only values from 1 to 31 ($1E_{hex}$) are valid for USS addressing. If you set values above 31, the set value is interpreted as "0".
- If the address 0 or an address above 31 is set using the address switch, the value in parameter p2021 defines the USS address.

You will find additional information in the manual for your converter.

Parameters to set communication via USS

Setting	Parameter	Comment
Fieldbus protocol selection	p2030 = 6 (USS (X140))	-
Baud rate	p2020 = 8, 38400 bit/s	-
Drive object that receives the PZD[1)]	p0978[0]	USS PZD go to the drive object that you entered under p0978[0] "List of drive objects".
PKW addressee[1)]	p2035	USS PKW address the drive object that you entered under p2035 "Fieldbus interface USS PKW drive object number".
Fieldbus interface USS PZD number	p2022 = 2	Setting the number of 16-bit words in the PZD part of the USS telegram
Fieldbus interface USS PKW number	p2023 = 127	Setting the number of 16-bit words in the PKW part of the USS telegram
Fieldbus error statistics	r2029	Displaying receive errors at the fieldbus interface
Fieldbus monitoring time	p2040 = 100 ms	The more slaves that are connected in the network, the longer you need to set the fieldbus monitoring time. If process data is not transferred within one cycle of the fieldbus monitoring time, the converter shuts down with fault F01910.

1) The factory settings of these parameters have been selected such that the USS communication extends to the drive object of the control.

A.1.7.2 Telegram structure

Overview

A USS telegram comprises a series of elements with a defined sequence. Each element contains 11 bits.

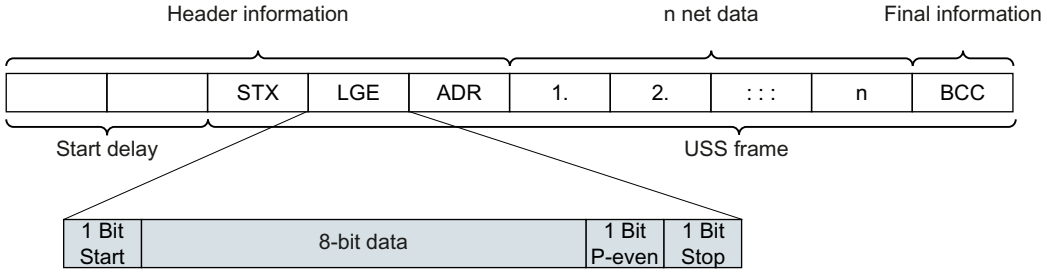


Figure A-53 Structure of a USS telegram

Telegram part	Description		
Start delay / response delay	There is always a start and/or response delay between 2 telegrams. Telegram monitoring (Page 246)		
STX	An ASCII character (02 hex) indicates the beginning of the message.		
LGE	The telegram length "LGE" is calculated as follows: LGE = user data (n bytes) + ADR (1 byte) + BCC (1 byte)		
ADR	7 6 5 4 3 2 1 0 Special telegram | Mirror telegram | Broadcast bit | Address		
	Bit 7	= 0	Normal data exchange
		= 1	Transferring telegrams that require a net data structure different from the device profile.
	Bit 6	= 0	Normal data exchange
		= 1	Testing the bus connection The converter returns the telegram unchanged to the master.
	Bit 5	= 0	Normal data exchange
		= 1	Not supported by the converter.
	Bits 0 ... 4		Address of the converter
User data	Specify user data of telegram (Page 237)		
BCC	Checksum (exclusive or) across all telegram bytes – with the exception of BCC		

A.1.7.3 Specify user data of telegram

Overview

The user data of the telegram consist of the following elements:

- Parameter channel (PKW) for writing and reading parameter values
- Process data (PZD) for controlling the drive

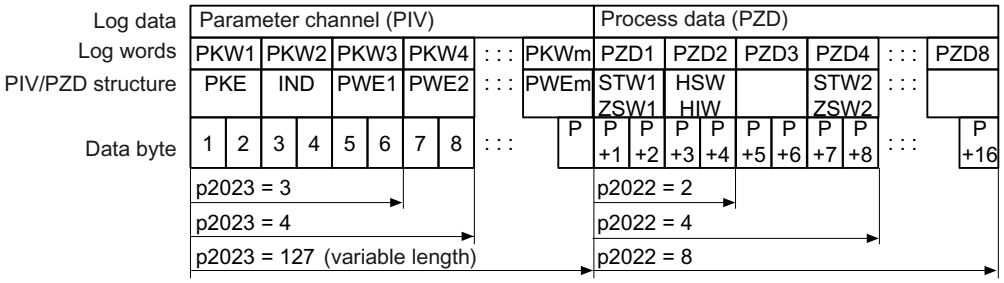


Figure A-54 USS telegram - user data structure

Function description

Parameter channel

You specify the length of the parameter channel in parameter p2023:

- p2023 = 0
  No parameter values are transferred with this setting.
- p2023 = 3
  Select this setting if you only want to read or write 16-bit data or alarm messages.
- p2023 = 4
  If you want to read or write 32-bit values (for example indexed parameters or bit parameters, e.g. r0722.2), this setting is required. In this case, the send or receive telegram always contains four words, even if only three would be required. The values are entered right-justified in the 4th word.
- p2023 = 127
  If you set p2023 = 127 (variable length), the send and response telegrams are exactly as long as the task requires.

Process data

Parameter p2022 defines the length for the process data. You can transfer up to eight process data items in one telegram (p2022 = 0 ... 8). For p2022 = 0, no process data is transferred.

Parameters

Parameter	Description	Factory setting
p2022	Fieldbus interface USS PZD number	2
p2023	Fieldbus interface USS PKW number	127

A.1.7.4 USS parameter channel

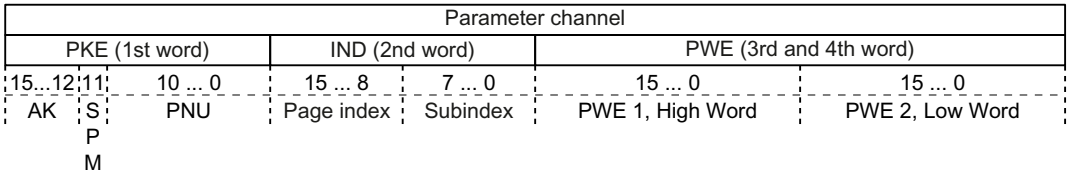
Structure of the parameter channel

Depending on the setting in p2023, the parameter channel has a fixed length of 3 or 4 words, or a variable length, depending on the length of the data to be transferred.

The 1st and 2nd words contain the parameter number and index as well as the type of job (read or write). The other words of the parameter channel contain parameter contents. The parameter contents can be 8-bit values, 16-bit values (such as baud rate) or 32-bit values (e.g. CO parameters). The parameter contents are entered right justified in the word with the highest number. Words that are not required are assigned 0.

Bit 11 in the 1st word is reserved and is always assigned 0.

The diagram shows a parameter channel that is four words long.



You can find examples of telegrams at the end of this section.

Function description

AK: Request and response ID

Table A-59 Request identifiers, control → converter

AK	Description	Response identifier	
		Positive	Negative
0	No request	0	7 / 8
1	Request parameter value	1 / 2	7 / 8
2	Change parameter value (word)	1	7 / 8
3	Change parameter value (double word)	2	7 / 8
4	Request descriptive element[1)]	3	7 / 8
6 [2)]	Request parameter value (field)[1)]	4 / 5	7 / 8
7 [2)]	Change parameter value (field, word)[1)]	4	7 / 8
8 [2)]	Change parameter value (field, double word)[1)]	5	7 / 8
9	Request number of field elements	6	7 / 8

1) The required element of the parameter is specified in IND (2nd word).

2) The following request identifiers are identical: 1 ≡ 6, 2 ≡ 7 and 3 ≡ 8. Use identifiers 6, 7, and 8.

Table A-60 Response identifiers, converter → control

AK	Description
0	No response
1	Transfer parameter value (word)
2	Transfer parameter value (double word)
3	Transfer descriptive element[1)]
4	Transfer parameter value (field, word)[2)]
5	Transfer parameter value (field, double word)[2)]
6	Transfer number of field elements
7	Converter cannot process the request. In the most significant word of the parameter channel, the converter sends an error number to the control, refer to the following table.
8	No master controller status / no authorization to change parameters of the parameter channel interface

1) The required element of the parameter is specified in IND (2nd word).

2) The required element of the indexed parameter is specified in IND (2nd word).

Table A-61 Error numbers for response identifier 7

No.	Description
00 hex	**Inadmissible parameter number** Access to a parameter that does not exist
01 hex	**Parameter value cannot be changed** Change request for a parameter value that cannot be changed
02 hex	**Upper or lower value limit exceeded** Change request with value outside value limits
03 hex	**Incorrect subindex** Access to a subindex that does not exist
04 hex	**No array** Access with subindex to non-indexed parameter
05 hex	**Incorrect data type** Change request with a value that does not match the data type of the parameter
06 hex	**Setting not permitted, only reset** Change request with a value not equal to 0 without permission
07 hex	**Descriptive element cannot be changed** Change request to a descriptive element that cannot be changed
0B hex	**No master control** Change request with no master control, see also p0927
0C hex	**Keyword missing**
11 hex	**Request cannot be executed due to operating status** Access is temporarily not possible for unspecified reasons.
14 hex	**Inadmissible value** Change request with a value that is within the limits but which is inadmissible for other permanent reasons, i.e. a parameter with defined individual values

No.	Description
65 hex	**Parameter number is currently deactivated** Dependent on the operating status of the converter
66 hex	**Channel width is insufficient** Communication channel is too small for response
68 hex	**Inadmissible parameter value** The parameter can only assume certain values
6A hex	**Request not included / task is not supported.** The valid request identifiers can be found in the table "Request identifiers control → converter"
6B hex	**No change access for enabled controller**. The operating status of the converter prevents a parameter change
86 hex	**Write access only for commissioning (p0010 = 15)** The operating status of the converter prevents a parameter change
87 hex	**Know-how protection active, access locked**
C8 hex	**Change request below currently valid limit** Change request for a value that, although within "absolute" limits, is below the currently valid lower limit
C9 hex	**Change request above currently valid limit** Example: A parameter value is too large for the converter rating
CC hex	**Change request not permitted** Change is not permitted as the access code is not available

PNU (parameter number) and page index

Parameter number	PNU	Page index
0000 ... 1999	0000 ... 1999	0 hex
2000 ... 3999	0000 ... 1999	80 hex
6000 ... 7999	0000 ... 1999	90 hex
8000 ... 9999	0000 ... 1999	20 hex
10000 ... 11999	0000 ... 1999	A0 hex
20000 ... 21999	0000 ... 1999	50 hex
29000 ... 29999	0000 ... 1999	70 hex
30000 ... 31999	0000 ... 1999	F0 hex
60000 ... 61999	0000 ... 1999	74 hex

Subindex

For indexed parameters, the parameter index is located in the subindex as a hexadecimal value.

PWE: Parameter value or connector

Parameter values or connectors can be located in the PWE.

Table A-62 Parameter value or connector

<table>
<tr><th></th><th>PWE 1</th><th colspan="3">PWE 2</th></tr>
<tr><td rowspan="4">Parameter value</td><td>Bits 15 ... 0</td><td colspan="2">Bits 15 ... 8</td><td>Bit 7 ... 0</td></tr>
<tr><td>0</td><td colspan="2">0</td><td>8-bit value</td></tr>
<tr><td>0</td><td colspan="3">16-bit value</td></tr>
<tr><td colspan="4">32-bit value</td></tr>
<tr><td rowspan="2">Connector</td><td>Bit 15 ... 0</td><td>Bit 15 ... 10</td><td colspan="2">Bit 9 ... 0</td></tr>
<tr><td>Number of the connector</td><td>3F hex</td><td colspan="2">The index or bit field number of the connector</td></tr>
</table>

Example

Read request: Read out memory card serial number (p7843[2])

To obtain the value of the indexed parameter p7843, you must fill the telegram of the parameter channel with the following data:

- **PKE, bits 12 ... 15 (AK): = 6** (request parameter value (field))
- **PKE, bits 0 ... 10 (PNU): = 1843** (parameter number without offset)
  Parameter number = PNU + offset (page index)
  (7843 = 1843 + 6000)
- **IND, bits 8 ... 15 (subindex): = 2** (index of parameter)
- **IND, bits 0 ... 7 (page index): = 90 hex** (offset 6000 corresponds to 90 hex)
- As you want to read the parameter value, words 3 and 4 in the parameter channel are irrelevant for requesting the parameter value. Therefore assign, for example, the value 0 to words 3 and 4.

<table>
<tr><th colspan="8">Parameter channel</th></tr>
<tr><td colspan="3">PKE, 1st word</td><td colspan="2">IND, 2nd word</td><td>PWE1 - high, 3rd word</td><td colspan="2">PWE2 - low, 4th word</td></tr>
<tr><td>15...12</td><td>11</td><td>10 ... 0</td><td>15 ... 8</td><td>7 ... 0</td><td>15 ... 0</td><td>15 ... 10</td><td>9 ... 0</td></tr>
<tr><td>AK</td><td></td><td>Parameter number</td><td>Subindex</td><td>Page index</td><td>Parameter value</td><td>Drive object</td><td>Index</td></tr>
<tr><td>0 1 1 0</td><td>0</td><td>1 1 1 0 0 1 1 0 0 0 1</td><td>0 0 0 0 0 0 1 0</td><td>1 0 0 1 0 0 0 0</td><td>0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0</td><td>0 0 0 0 0 0</td><td>0 0 0 0 0 0 0 0 0 0</td></tr>
</table>

Figure A-55 Telegram for a read request from p7843[2]

Parameter number

Parameter numbers < 2000	PNU = parameter number. Write the parameter number into the PNU (PKE bit 10 ... 0).
Parameter numbers ≥ 2000	PNU = parameter number - offset. Write the parameter number minus the offset into the PNU (PKE bit 10 ... 0). Write the offset in the page index (IND bit 15 ... 8).

Table A-63 Offset and page index of the parameter numbers

Parameter number	Offset	Page index								
		Hex	Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8
0000 ... 1999	0	0 hex	0	0	0	0	0	0	0	0
2000 ... 3999	2000	80 hex	1	0	0	0	0	0	0	0
6000 ... 7999	6000	90 hex	1	0	0	1	0	0	0	0
8000 ... 9999	8000	20 hex	0	0	1	0	0	0	0	0
10000 ... 11999	10000	A0 hex	1	0	1	0	0	0	0	0
20000 ... 21999	20000	50 hex	0	1	0	1	0	0	0	0
29000 ... 29999	28000	70 hex	0	1	1	1	0	0	0	0
30000 ... 31999	30000	F0 hex	1	1	1	1	0	0	0	0
60000 ... 61999	60000	74 hex	0	1	1	1	0	1	0	0

Indexed parameters

For indexed parameters, you must write the index as a hexadecimal value into the subindex (IND bits 7 ... 0).

Parameter contents

Parameter contents can be parameter values or connector parameters. For connector parameters you require 2 words.

Enter the parameter value in the parameter channel right-justified as follows:

- 8-bit values Low word, bits 0 ... 7 Bits 8 ... 15 are zero.
- 16-bit values Low word, bits 0 ... 15
- 32-bit values Low word and high word

Enter a connector parameter right-justified as follows:

- Number of the connector parameter — High word
- Drive object of the connector parameter — Low word, bits 10 ... 15
- The index or bit field number of the connector parameter — Low word, bits 0 ... 9

Telegram examples, length of the parameter channel = 4

Read request: Read out memory card serial number (p7843[2])

To obtain the value of the indexed parameter p7843, you must fill the telegram of the parameter channel with the following data:

- **PKE, bits 12 ... 15 (AK) = 6** (request parameter value (field))
- **PKE, bits 0 ... 10 (PNU) = 1843** (parameter number without offset)
  Parameter number = PNU + offset (page index)
  (7841 = 1843 + 6000)
- **IND, bits 8 ... 15 (page index) = 90 hex** (offset 6000 corresponds to 90 hex)

- **IND, bits 0 ... 7 (subindex) = 2** (index of parameter)
- As you want to read the parameter value, words 3 and 4 in the parameter channel are irrelevant for requesting the parameter value. Therefore assign, for example, the value 0 to words 3 and 4.

Parameter channel							
PKE (1st word)			IND, 2nd word		PWE1 - high, 3rd word	PWE2 - low, 4th word	
15...12	11	10 ... 0	15 ... 8	7 ... 0	15 ... 0	15 ... 10	9 ... 0
AK		Parameter number	Page index	Subindex	Parameter value	Drive Object	Index
0 1 1 0	0	1 1 1 0 0 1 1 0 0 0 1	1 0 0 1 0 0 0 0	0 0 0 0 0 0 1 0	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0 0 0 0 0 0	0 0 0 0 0 0 0 0 0 0

Figure A-56 Telegram for a read request from p7843[2]

Write request: Changing the automatic restart mode (p1210)

Parameter p1210 defines the automatic restart mode:

- **PKE, bit 12 ... 15 (AK): = 7** (change parameter value (field, word))
- **PKE, bit 0 ... 10 (PNU): = 4BA hex** (1210 = 4BA hex, no offset, as 1210 < 1999)
- **IND, bit 8 ... 15 (page index): = 0 hex** (offset 0 corresponds to 0 hex)
- **IND, bit 0 ... 7 (subindex): = 0 hex** (parameter is not indexed)
- **PWE1, bit 0 ... 15: = 0 hex**
- **PWE2, bit 0 ... 15: = 1A hex** (26 = 1A hex)

Parameter channel						
PKE, 1st word			IND, 2nd word		PWE1 - high, 3rd word	PWE2 - low, 4th word
15...12	11	10 ... 0	15 ... 8	7 ... 0	15 ... 0	15 ... 0
AK		Parameter number	Page index	Subindex	Parameter value (bit 16 ... 31)	Parameter value (bit 0 ... 15)
0 1 1 1	0	1 0 0 1 0 1 1 1 0 1 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0 0 0 0 1 1 0 1 0

Figure A-57 Telegram, to activate the automatic restart with p1210 = 26

Write request: Assign digital input 2 with the function ON/OFF1 (p0840[1] = 722.2)

In order to link digital input 2 with ON/OFF1, you must assign parameter p0840[1] (source, ON/OFF1) the value 722.2 (DI 2). To do this, you must fill the telegram of the parameter channel as follows:

- **PKE, bit 12 ... 15 (AK): = 7 hex** (change parameter value (field, word))
- **PKE, bit 0 ... 10 (PNU): = 348 hex** (840 = 348 hex, no offset, as 840 < 1999)
- **IND, bit 8 ... 15 (page index): = 0 hex** (offset 0 corresponds to 0 hex)
- **IND, bit 0 ... 7 (subindex): = 1 hex** (command data set CDS1 = index1)
- **PWE1, bit 0 ... 15**: = **2D2 hex** (722 = 2D2 hex)
- **PWE2, bit 10 ... 15: = 3f hex** (drive object - for SINAMICS G120 always 63 = 3f hex)
- **PWE2, bit 0 ... 9: = 2 hex** (index or bit number of the parameter: DI 2 = r0722.2)

Parameter channel							
PKE, 1st word			IND, 2nd word		PWE1 - high, 3rd word	PWE2 - low, 4th word	
15...12	11	10 ... 0	15 ... 8	7 ... 0	15 ... 0	15 ... 10	9 ... 0
AK		Parameter number	Page index	Subindex	Parameter value	Drive Object	Index
0 1 1 1	0	0 1 1 0 1 0 0 1 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 1	0 0 0 0 0 0 1 0 1 1 0 1 0 0 1 0	1 1 1 1 1 1	0 0 0 0 0 0 0 0 1 0

Figure A-58 Telegram, to assign DI 2 with ON/OFF1

A.1.7.5 USS process data channel (PZD)

Function description

The process data channel (PZD) contains the following data depending on the transmission direction:

- Control words and setpoints for the slave
- Status words and actual values for the master

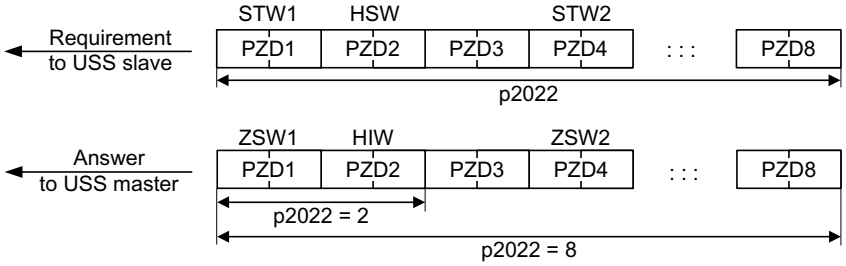


Figure A-59 Process data channel

With the exception of telegram 999 (free interconnection), the telegrams use the word-by-word transfer of send and receive data (r2050/p2051).

If you require an individual telegram for your application (e.g. for transferring double words), you can adapt one of the predefined telegrams using parameters p0922 and p2079. For details, please refer to the List Manual, function diagrams 2420 and following.

Control word 1 (STW1)

Bit	Meaning		Explanation	Signal interconnection in the converter
	Telegram 20	All other telegrams		
0	0 = OFF1		The motor brakes with the ramp-down time p1121 of the ramp-function generator. The converter switches off the motor at standstill.	p0840[0] = r2090.0
	0 → 1 = ON		The converter goes into the "ready" state. If, in addition, bit 3 = 1, the converter switches on the motor.	
1	0 = OFF2		Switch off the motor immediately, the motor then coasts down to a standstill.	p0844[0] = r2090.1
	1 = No OFF2		The motor can be switched on (ON command).	
2	0 = Quick stop (OFF3)		Fast stopping The motor brakes with the OFF3 ramp-down time p1135 down to standstill.	p0848[0] = r2090.2
	1 = No quick stop (OFF3)		The motor can be switched on (ON command).	
3	0 = Inhibit operation		Immediately switch-off motor (cancel pulses).	p0852[0] = r2090.3
	1 = Enable operation		Switch-on motor (pulses can be enabled).	

Bit	Meaning		Explanation	Signal interconnection in the converter
	Telegram 20	All other telegrams		
4	0 = Disable RFG		The converter immediately sets its ramp-function generator output to 0.	p1140[0] = r2090.4
	1 = Do not disable RFG		The ramp-function generator can be enabled.	
5	0 = Stop RFG		The output of the ramp-function generator stops at the actual value.	p1141[0] = r2090.5
	1 = Enable RFG		The output of the ramp-function generator follows the setpoint.	
6	0 = Inhibit setpoint		The converter brakes the motor with the ramp-down time p1121 of the ramp-function generator.	p1142[0] = r2090.6
	1 = Enable setpoint		Motor accelerates with the ramp-up time p1120 to the setpoint.	
7	0 → 1 = Acknowledge faults		Acknowledge fault. If the ON command is still active, the converter switches to the "switching on inhibited" state.	p2103[0] = r2090.7
8, 9	Reserved			
10	0 = No control via PLC		Converter ignores the process data from the fieldbus.	p0854[0] = r2090.10
	1 = Control via PLC		Control via fieldbus, converter accepts the process data from the fieldbus.	
11	1 = Direction reversal		Invert setpoint in the converter.	p1113[0] = r2090.11
12	Not used			
13	---[1)]	1 = MOP up	Increase the setpoint saved in the motorized potentiometer.	p1035[0] = r2090.13
14	---[1)]	1 = MOP down	Reduce the setpoint saved in the motorized potentiometer.	p1036[0] = r2090.14
15	CDS bit 0	Reserved	Changes over between settings for different operation interfaces (command data sets).	p0810 = r2090.15

[1)] If you change over from another telegram to telegram 20, then the assignment of the previous telegram is kept.

Status word 1 (ZSW1)

Bit	Meaning		Remarks	Signal interconnection in the converter
	Telegram 20	All other telegrams		
0	1 = Ready for switching on		Power supply switched on; electronics initialized; pulses locked.	p2080[0] = r0899.0
1	1 = Ready		Motor is switched on (ON/OFF1 = 1), no fault is active. With the command "Enable operation" (STW1.3), the converter switches on the motor.	p2080[1] = r0899.1
2	1 = Operation enabled		Motor follows setpoint. See control word 1, bit 3.	p2080[2] = r0899.2

Bit	Meaning		Remarks	Signal interconnection in the converter
	Telegram 20	All other telegrams		
3	1 = Fault active		The converter has a fault. Acknowledge fault using STW1.7.	p2080[3] = r2139.3
4	1 = OFF2 inactive		Coast down to standstill is not active.	p2080[4] = r0899.4
5	1 = OFF3 inactive		Quick stop is not active.	p2080[5] = r0899.5
6	1 = Switching on inhibited active		It is only possible to switch on the motor after an OFF1 followed by ON.	p2080[6] = r0899.6
7	1 = Alarm active		Motor remains switched on; no acknowledgement is necessary.	p2080[7] = r2139.7
8	1 = Speed deviation within the tolerance range		Setpoint / actual value deviation within the tolerance range.	p2080[8] = r2197.7
9	1 = Master control requested		The automation system is requested to accept the converter control.	p2080[9] = r0899.9
10	1 = Comparison speed reached or exceeded		Speed is greater than or equal to the corresponding maximum speed.	p2080[10] = r2199.1
11	1 = current or torque limit reached	1 = torque limit reached	Comparison value for current or torque has been reached or exceeded.	p2080[11] = r0056.13 / r1407.7
12	---[1]	1 = Holding brake open	Signal to open and close a motor holding brake.	p2080[12] = r0899.12
13	0 = Alarm, motor overtemperature		--	p2080[13] = r2135.14
14	1 = Motor rotates clockwise		Internal converter actual value > 0	p2080[14] = r2197.3
	0 = Motor rotates counter-clockwise		Internal converter actual value < 0	
15	1 = CDS display	0 = Alarm, converter thermal overload	--	p2080[15] = r0836.0 / r2135.15

[1] If you change over from another telegram to telegram 20, then the assignment of the previous telegram is kept.

A.1.7.6 Telegram monitoring

Function description

You require the telegram runtimes in order to set the telegram monitoring. The character runtime is the basis of the telegram runtime:

Table A-64 Character runtime

Baud rate in bit/s	Transmission time per bit	Character run time (= 11 bits)
9600	104.170 µs	1.146 ms
19200	52.084 µs	0.573 ms

Baud rate in bit/s	Transmission time per bit	Character run time (= 11 bits)
38400	26.042 µs	0.286 ms
57600	17.361 µs	0.191 ms
115200	8.681 µs	0.095 ms

The telegram runtime is longer than just purely adding all of the character runtimes (=residual runtime). You must also take into consideration the character delay time between the individual characters of the telegram.

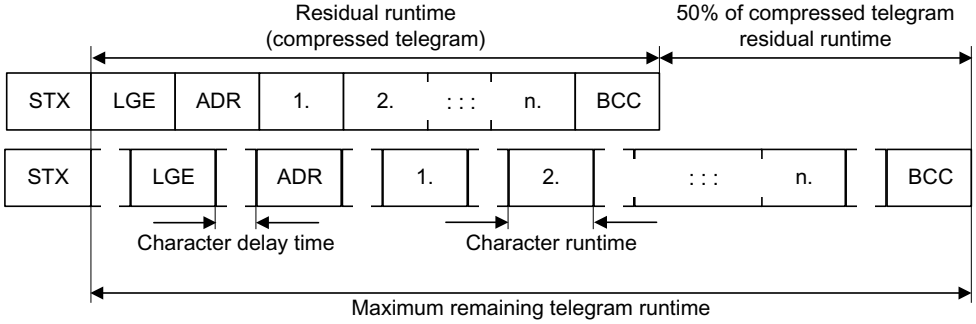


Figure A-60 Telegram runtime as the sum of the residual runtime and character delay times

The total telegram runtime is always less than 150% of the pure residual runtime.

Before each request telegram, the master must maintain the start delay. The start delay must be > 2 × character runtime.

The slave only responds after the response delay has expired.

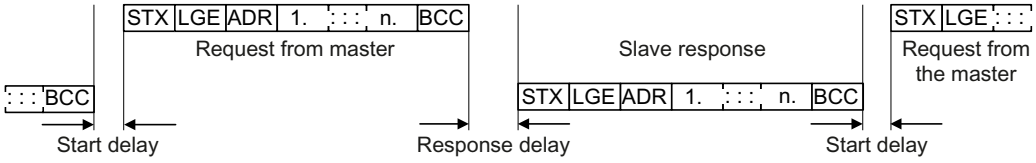


Figure A-61 Start delay and response delay

Table A-65 Start delay

Baud rate in bit/s	Transmission time per character (= 11 bits)	Min. start delay
9600	1.146 ms	> 2.291 ms
19200	0.573 ms	> 1.146 ms
38400	0.286 ms	> 0.573 ms
57600	0.191 ms	> 0.382 ms
115200	0.095 ms	> 0.191 ms

The character delay time must be shorter than the start delay.

Telegram monitoring of the master

With your USS master, we recommend that the following times are monitored:

- Response delay:
  Response time of the slave to a request from the master
  The response delay must be < 20 ms, but longer than the start delay
- Telegram runtime:
  Transmission time of the response telegram sent from the slave

Telegram monitoring of the converter

The converter monitors the time between two requests of the master. Parameter p2040 defines the permissible time in ms. If a time p2040 ≠ 0 is exceeded, then the converter interprets this as telegram failure and responds with fault F01910.

150% of the residual runtime is the guide value for the setting of p2040, i.e. the telegram runtime without taking into account the character delay times.

For communication via USS, the converter checks bit 10 of the received control word 1. If the bit is not set when the motor is switched on ("Operation"), the converter responds with fault F07220.

Parameters

Parameter	Description	Factory setting
p2040	Fieldbus interface monitoring time	1 000 ms

A.1.8 Time synchronization between the control and converter

In the factory setting, SINAMICS drives use an operating hours counter. Based on the operating hours, the SINAMICS drive saves alarms and warnings that occur. Using this method, it is not possible to have a comparable timestamp between various converters.

In order to obtain a comparable timestamp between several converters, you must change over the operating hours counting to time in the UTC format and synchronize with the time master (control system).

This means that the events of all bus nodes, which are synchronized with the control system time, can be referenced with one another.

Benefits: Improved diagnostic options by having a comparable time stamp of the bus nodes involved.

Converters provide the following options to synchronize the time:

Synchronization type	Accuracy
Basic synchronization	approx. 100ms
Synchronization using ping compensation for non-isochronous communication	approx. 10 ms
Synchronization using ping compensation for isochronous communication	approx. 1 ms

Principle of operation of time synchronization

Basic synchronization

The control system transfers the time to the converter at time intervals that you specify in the control system. Transfer is realized acyclically in the UTC format. The converter accepts this time as soon as transfer has been completed without correcting the transfer duration. The converter logs alarms and warnings based on this time.

Time synchronization with ping compensation

At intervals that you specify in the control system, the control system sends a ping (a positive signal edge) cyclically to the converter. Simultaneously, in acyclic operation, the device sends the time in the UTC format in what is known as "snap".

As soon as the ping has been received in the drive, a timer starts which measures the time until the snap has been completely transferred. The drive accepts the time that the snap transfers. It then corrects it by the time that has expired between receiving the ping and the complete transfer of the snap.

If the snap has not been transferred within 5 s after receiving the ping, then this synchronization cycle is not used.

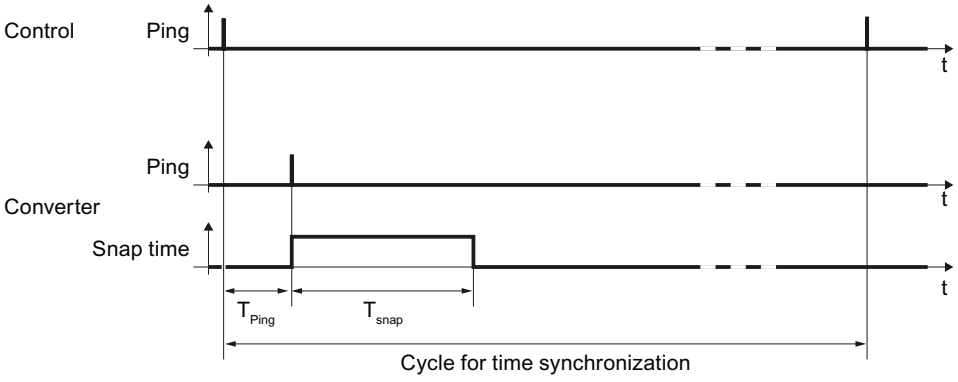


Figure A-62 Ping snap

Differences for isochronous and non-isochronous communication:

Communication	Description
Isochronous	The ping compensation value is determined in the converter.
not isochronous	You can influence the accuracy of the ping compensation using the PZD sampling time (p2048).

A.1.8.1 Setting SINAMICS time synchronization

Setting time synchronization

1. Using p3100, changeover the time format from operating hours into the UTC format (see "Changing the time format").
2. Set the synchronization technique:
   - Basic synchronization (p3103 = 2)
   - Time synchronization with ping compensation (p3103 = 0)
3. Using p3104, set the ping source:
   - If you are working with one of the telegrams 390, 391 or 392, then the source of the ping (p3104) is internally connected with bit 1 of the CU control word (DO1:CU_STW.1). In this case, parameter p3104 is blocked.
   - If you are using a free telegram (999), interconnect the ping source (p3104) via BICO in the control word.
   - If you are working with CANopen, interconnect a free bit in the CANopen control word with p3104 via a BICO connection.

Result:

After time synchronization, the current time is obtained from the time transferred by the time master plus the necessary delay time associated with the transfer (ping-snap time).

The actual UTC time is displayed in the drive system using r3102.

At certain intervals, synchronization (according to the same technique) is repeated (depending on the setting in the time master).

If a previously defined tolerance window is exceeded, then alarm A01099 is output. Define the tolerance window for time synchronization using p3109. If alarm A01099 occurs, then generally the synchronization interval is too long.

In this case, reduce the synchronization interval in your control system.

Changing the time format

The time format is entered via parameter p3100. This parameter cannot be changed online To change the value, proceed as follows:

1. Connect Startdrive ONLINE with the converter.
2. Carry out an upload using the "Load from device" function.
3. In Startdrive, exit the ONLINE mode.
4. Offline, make the setting p3100 = 1.
5. Reactivate the ONLINE mode.
6. Carry out a parameter download ("Load to device").
7. Save the settings in a non-volatile fashion on the memory card of the drive.
   You have now changed over the converter time format to the UTC format.

Application example

You can find an application example for SINAMICS time synchronization in the SIEMENS "Industry Online Support":

Time synchronization example (https://support.industry.siemens.com/cs/de/en/view/88231134)

A.1.8.2 Messages and parameters

Faults and alarms

Note

You can find the description of faults and alarms in the converter List Manual.

Fault number	Message
A01099	UTC synchronization tolerance violated

Overview of important parameters

Note

For a description of the parameters, see the converter List Manual.

Parameter	Description
p2048	IF1 PROFIdrive PZD sampling time
p3100	RTC time stamp mode
p3101[0...1]	Set UTC time
r3102[0...1]	Display UTC time
p3103	UTC synchronization technique
p3104	BI: UTC PING synchronization
r3107[0...3]	UTC synchronization time out of tolerance
r3108[0...1]	UTC synchronization deviation
p3109	UTC synchronization tolerance
p3116	BI: Suppress automatic acknowledgment

A.2 Web server

Overview

The web server is a web-based commissioning tool for SINAMICS S120 converters and provides information on a connected SINAMICS S120 converter via its web pages.

You can open the web server via the Internet browser of your commissioning device.

Total memory size

The sum of the data and files stored in the web server must not exceed the total memory size of 100 MB. The total size of the saved data and files has an impact on the backup times. The larger the data quantity, the longer the backup takes.

Delimitation of contents

The display areas "System > Files", "System > User area configuration" and "User area" are described in detail in the documentation specified below and are not described in this chapter.

- S120 web server - Creating user-defined web pages (https://support.industry.siemens.com/cs/ww/en/view/68691599)
- S120 web server – User-defined sample pages (https://support.industry.siemens.com/cs/ww/en/view/78388880)

Configuration

The web server is already activated in the factory settings of the converter. You perform configuration of the web server either directly in the web server (see Chapter "System settings (Page 312)") or in the Startdrive engineering tool.

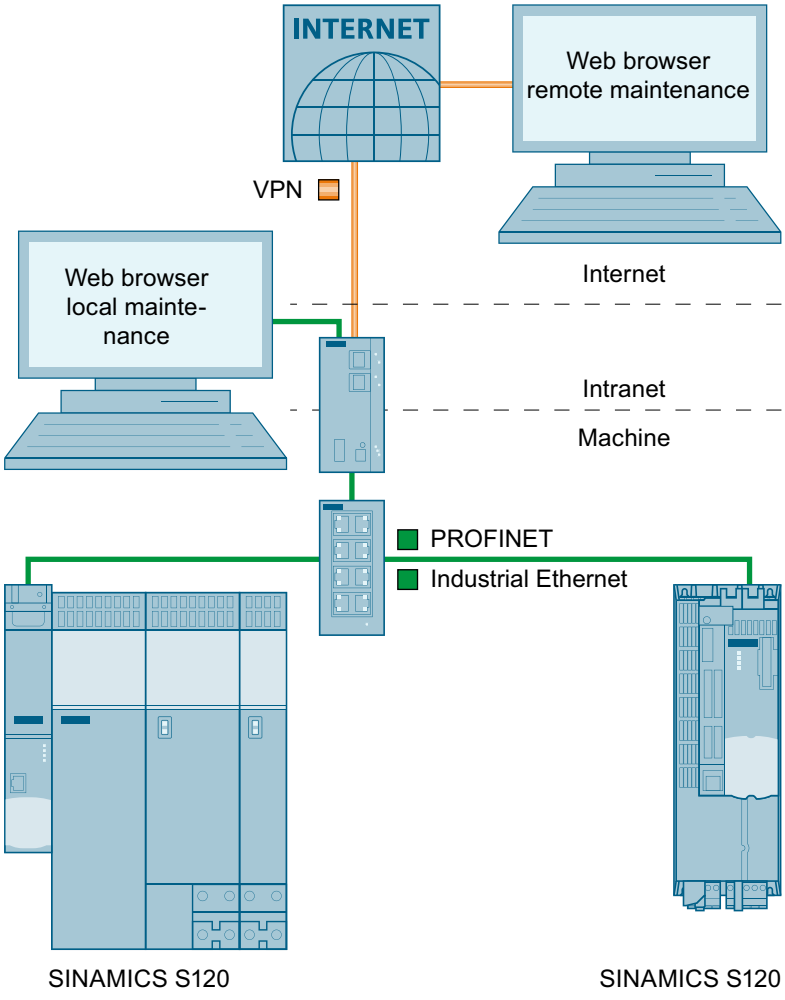


Figure A-63 Web server structure

Additional information

Additional information regarding configuring the web server in the Startdrive engineering tool is provided in the SINAMICS S120 Commissioning Manual with Startdrive.

Communication

The web server supports unencrypted communication via the HTTP protocol as well as encrypted communication via the HTTPS protocol.

Additional information

You can find more information on configuring the IP connection in Chapter "Configuring the IP connection (Page 318)".

Access rights

The normal SINAMICS protection mechanisms apply to the web server, including password protection. The permanently defined user roles with the assigned access rights offer additional security.

User roles

The user roles in the web server have the following features and characteristics:

- **Administrator:**
  - Advanced access rights
    The advanced access rights authorize the "Administrator" user to expand the access rights of the "SINAMICS" user role.
  - Intended for commissioning tasks
    The most important commissioning tasks include creating parameter lists and changing parameter values in existing parameter lists.
- **SINAMICS:**
  - Restricted access rights
  - Intended for diagnostics tasks

Additional information

You will find information about the user roles and their access rights to the web server functions in Chapter "Access rights (Page 258)".

A.2.1 Fundamentals

A.2.1.1 Supported Internet browsers

Overview

You can display the content of the web server either on a PC/laptop screen, a tablet PC or a smartphone.

List of supported Internet browsers

The web server integrated in the converter supports the following web browsers:

Commissioning device	Operating system	Supported browsers
PG/PC	Windows (as of Version 7)[1)]	• Microsoft Internet Explorer (Version 11) • Microsoft Edge (Version 14) • Mozilla Firefox (Version 62) • Google Chrome (Version 69)[2)]
Tablet, Smartphone	Apple iOS (from Version 12.0)	• Google Chrome (Version 69) • Safari (Version 12.0)
	Android (from Version 4.4.4)	• Google Chrome (Version 69)

1) We recommend the use of Windows 10, Version 1803, dated April 2018 or later.

2) We recommend the use of Google Chrome in the supported version 69.

Reloading pages

If the web server does not respond, or if buttons are inactive or are not labeled, although the converter is not fully utilized with internal calculations, load the web server pages again as follows:

- With the PG/PC via <F5>
- With the smartphone or tablet via ↻

A.2.1.2 Accessing the web server

For access to the web server, the following interfaces are available on the converter:

- Service interface X127 (standard)
- PROFINET interface X150

Access via service interface X127

The web server is accessed per default via the service interface X127.

Features

- Preset IP address: 169.254.11.22
- Preset subnet mask: 255.255.0.0

- Access via the service interface is **activated by default** in the web server.
- Data transfer via HTTP (factory setting) and HTTPS connection possible.

NOTICE
Risk of software manipulation with HTTP connection The HTTP protocol transfers data without encryption. This facilitates, for example, password theft and can lead to data manipulation by unauthorized parties and thus to damage. • Limit access to HTTPS connections so that all data is transferred in encrypted form.

Interface X127 can also be connected to an external WLAN access point, and from this an IP address can be sourced via DHCP. This is just a temporary situation, and is only used for commissioning and/or diagnostics with mobile devices. The subsequently described security notes must be carefully observed when doing this.

Additional notes on using the service interface

Note

Service interface X127 is intended for commissioning and diagnostics, which means that it must always be accessible (e.g. for service).

The following restrictions apply in addition:

- Only local access is permissible.
- No networking - or only local networking is permissible in a locked control cabinet.

If remote access to the control cabinet is required, additional safety measures need to be taken so that misuse through sabotage, unqualified data manipulation and eavesdropping on confidential data can be ruled out (see also Chapter "Industrial Security (Page 17)").

Access via PROFINET interface X150

Access to the web server is also possible via the PROFINET interface X150.

Features

- Access via the PROFINET interface is **deactivated by default** in the web server.
  The PROFINET interface can be activated using parameter p8984[1]. Because parameter p8984[1] is a BICO parameter, the interface can also be activated via a key-operated switch.
- Data transfer is only possible via an HTTPS connection.

Note

Security measures for communication via PROFINET

In accordance with the Defense in Depth concept, PROFINET must be isolated from the remaining plant network (see Chapter Industrial Security (Page 17)). Access to cables and possibly open connections must be implemented in a protected fashion, such as in a control cabinet.

Note

It is not permissible that the IP addresses of the service and PROFINET interfaces are in the same subnet (see Chapter "Access via service interface X127 (Page 255)").

Calling the web server

Procedure

Proceed as follows to call the web server:

1. Connect the converter to your commissioning device via the service interface X127.
2. Switch the converter on.
   The converter starts up.
3. Open the web browser in your commissioning device.
4. Call the web server using the converter IP address (e.g. 169.254.11.22).

A.2.1.3 Access protection

Overview

Access protection in the web server comprises the following protective measures:

- User roles
  Access to the converter is possible via two defined user roles ("Administrator" and "SINAMICS") with different access rights in the web server (see Chapter "Access rights (Page 258)").
  We recommend the creation of secure passwords for access to the SINAMICS S120 converter.
- Access rights to parameter lists
  Access rights to parameter lists in the web server are defined or changed by the "Administrator" user (see Chapter "Creating a parameter list (Page 306)" and "Changing the list properties (Page 309)").

Access rights

Overview

The following user roles are available for access to the web server:

- Administrator

Access rights	The "Administrator" user has full access to the converter data displayed in the web server.
Password	For access to the converter, assigning an administrator password is absolutely necessary (see Chapter "Setting or changing user accounts (Page 312)").

- SINAMICS

Access rights	The "SINAMICS" user has restricted access rights in the default settings of the web server.
Password	By default, a password is not assigned for the SINAMICS user. We recommend that a password is assigned to avoid access by unauthorized persons.

Configuring passwords

You can configure the passwords of the users "Administrator" and "SINAMICS" in the system settings of the web server with administrator rights (see Chapter "Assigning the administrator password (Page 262)").

Assignment of access rights

The access rights for the "Administrator" and "SINAMICS" users are assigned as follows in the default settings:

Display areas and functions		Administrator		SINAMICS	
		W/E	R	W/E	R
Home page	Password input	x		x	
Diagnostics	Drive objects and components	x		x	
	Messages > Search and filter	x		x	
	Messages > Acknowledge faults	x		x	
	Diagnostics buffer > Search and filter	x		x	
	Communication	x		x	
	Trace files	x		x	

Display areas and functions		Administrator		SINAMICS	
		W/E	R	W/E	R
Parameter	Create list	x		x	
	List properties > Access rights > Read parameter values	x		x[1]	
	List properties > Access rights > Change parameter values ... • ... Add parameters • ... Delete parameters • ... Change parameter values	x			x[2]
	List properties > Access rights > Change list • ... Enter / change list names • ... Delete list	x		x[1]	
	List properties > Change position of list	x		x	
Backup and restore	Back up parameters	x[3]			
	Restore parameters from file	x[3]			
	Restore factory settings	x[3]			
System	Settings > User accounts	x[3]			
	Settings > Configure IP connections	x[3]			
	Licenses	x			x
	Firmware update	x[3]			
Save changes (RAM to ROM)		x		x	
Call Support			x		x

W/E = Write/Edit, R = Read

1) The parameter lists generated by user "SINAMICS" are automatically assigned access rights "Read parameter values" and "Change list". The automatically assigned access rights can be extended or restricted by the "Administrator" user. The "Administrator" user can assign the access right "Change parameter values" to a parameter list created by the "SINAMICS" user and at the same time deactivate the automatically assigned access right "Change list". As a consequence, a "SINAMICS" user can change individual values in the corresponding parameter list; however, he cannot add additional parameters to the list or delete parameters that have already been added.

2) The function and the associated operating options are displayed for both users. However, the access rights for the function can only be assigned by user "Administrator".

3) The function and the associated operating options are not displayed for the "SINAMICS" user and are solely reserved for the "Administrator" user.

A.2.1.4 SINAMICS write and know-how protection

Function description

Write or know-how protection set in the STARTER or Startdrive commissioning tool is also effective for access via the web server. The set protective measure **cannot** be configured or deactivated in the web server.

If know-how protection is set, then no values are displayed in the parameter list of the web server; instead, a note referring to the fact that know-how protection is activated.

Additional information

- A description of SINAMICS write protection is provided in Chapter "Write protection (Page 327)".
- A description of SINAMICS know-how protection is provided in Chapter "Know-how protection (Page 329)".

A.2.1.5 Dialog screen forms in the web server

You make most of the important converter settings in the dialog screen forms of the web server. The web pages are as follows:

1 Navigation bar

2 Status bar

- Top: Device designation, drop-down list for the language selection and to log out, display of the security level
- Bottom: Name of the converter (if entered), status of the converter, fault and warning messages

3 Main window (depending on navigation)

Figure A-64 Example of a dialog screen

In some cases, you must make the parameter settings or read out values which can only be found in the parameter list of the converter. Additional information is provided in Chapter "Creating and adjusting the parameter list (Page 305)".

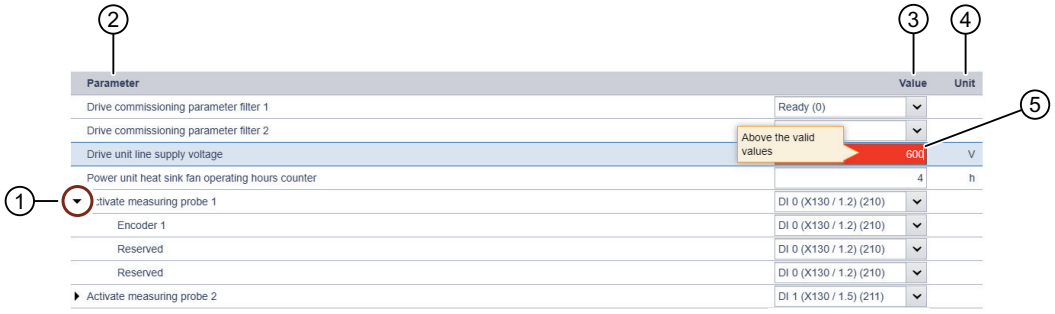
A.2.1.6 Changing parameter values

Overview

The parameters displayed in the web server are subdivided into adjustable parameters (p...) and display parameters (r...). The parameters are shown in the same way in parameter lists and dialog screen forms.

Adjustable parameters

You change the parameter values for adjustable parameters in the parameter lists and dialog screen forms by means of input fields ② or drop-down lists ③.



① Parameter (opened)
② "Parameter" column
③ "Value" column (values can be changed via drop-down lists or input fields.)
④ "Unit" column
⑤ Input field (invalid values are displayed with red background.)

Figure A-65 Example: Display of adjustable parameters

Input of invalid values

The web server responds to the input of invalid values in the following ways:

- If the input of an invalid value is confirmed with "Enter", a corresponding message is shown (e.g. "Value invalid") and the value is automatically set to the previously set value.
  The invalid value is not applied.
- If the input of an invalid value is confirmed with "Enter", the value is automatically set to the default value. If the previously set value differs from the default value, the previously set value is overwritten.
  The invalid value is not applied.

Display parameters

Display parameters are for information purposes only and cannot be changed.

A.2.1.7 Administrator password

Assigning the administrator password

Overview

For the first login to the web server, the assignment of an administrator password is mandatory.

When you have logged on successfully, you will receive advanced access to all web server functions as "Administrator" user. An overview of all web server functions and the assignment of access rights is provided in Chapter "Access rights (Page 258)".

Administrator password already assigned

If you have already been assigned an administrator password, then proceed as described in Chapter "User login (Page 264)".

You have forgotten the administrator password

If you as "Administrator" user have misplaced or forgotten your administrator password, there is no possibility in the web server to assign a new password. To create a new administrator password, proceed as described in Chapter "Password forgotten (Page 314)".

Requirements

- The converter has the factory settings.
  All web server data (passwords and settings) are lost if the converter is reset to the factory settings.

Procedure

Proceed as follows to assign an administrator password:

1. Switch the converter on.
2. Connect the commissioning device (PG/PC, tablet or smartphone) to service interface X127 on the converter using a LAN cable.

   Note

   Observe time window

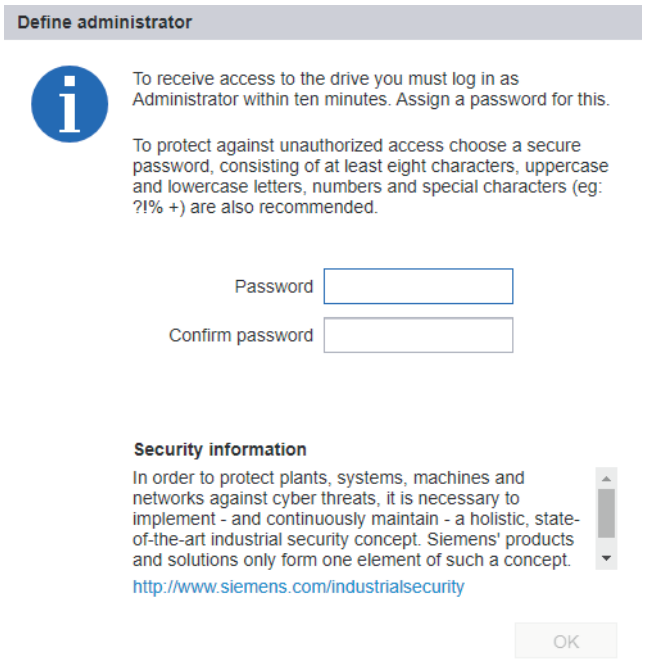
   Once you have connected the commissioning device with service interface X127 at the converter, assign a password within 10 minutes.

   If a password is not assigned within this time window, the display automatically switches to the login screen of the web server. To redisplay dialog "Define administrator", proceed as follows:

   - Switch the converter off and on again.
     OR
   - Withdraw the LAN cable from service interface X127, and then reinsert it into the service interface.

3. Open the browser in your commissioning device.

4. Call the web server using the converter IP address (e.g. 169.254.11.22).
   If you have not assigned a password, then the following dialog is displayed.



5. Enter an administrator password in the "Password" field.

Note

Secure passwords

To protect against unauthorized access, by a hacker, for example, select a secure password that comprises:

- At least 8 characters
- Uppercase and lowercase letters
- Numbers and special characters (e.g.: ?!%+ ...)

It is not permissible that the password is used elsewhere.

Note

Checking passwords

When passwords are entered, the converter only checks the password length. A check is not made for special characters or uppercase/lowercase letters!

6. Repeat the password in the "Confirm password" field.
   If the input is not identical in both fields, the "OK" button is not enabled.
7. Confirm the password that you entered with "OK".
   The display changes to the login page of the web server.
8. Log in using the administrator password.
9. Remember the password or store it in a secure place that cannot be accessed by unauthorized persons.

Changing the administrator password

Procedure

To change an existing administrator password, proceed as described in Chapter "Setting or changing user accounts (Page 312)".

A.2.1.8 User login

Overview

In order to be able to work with the web server, you must be logged in as "SINAMICS" or "Administrator" user.

You must be logged in as "Administrator" user to perform commissioning tasks.

Requirements

- You have already assigned a password for the "Administrator" user
  Additional information on assigning a password for an "Administrator" user is provided in Chapter "Assigning the administrator password (Page 262)".
- You have already assigned a password for the "SINAMICS" user.
  You can find additional information on assigning a password for the "SINAMICS" user in Chapter "Setting or changing user accounts (Page 312)".

Procedure

Proceed as follows to log into the web server:

1. Call the web server using the converter IP address (e.g. 169.254.11.22).
   The login page of the web server is displayed in the browser.
2. Enter the name of the user (Administrator or SINAMICS) in the "User name" field.
3. Then enter the password of the particular user.
4. Make sure that you have entered the user name and password correctly.
5. Click "Login".

You are logged into the web server.

A.2.1.9 User logout

Procedure

Proceed as follows to log out of the web server:

1. Click the user symbol in the status bar of the web server.
2. Click "Logout".
   If have changed the settings, a save prompt appears.
3. If you want to save the settings retentively, click "Save changes".
   The settings are saved retentively and you are logged out of the web server.
   OR
4. If you want to discard the settings, click "Log out without saving".
   The settings are discarded and you are logged out of the web server.

Automatic logout

Overview

If you do not perform any actions in the web server, you are automatically logged out after 10 minutes.

Settings made are **not** lost as a result of automatic logout. You must log in again to be able to access the web server.

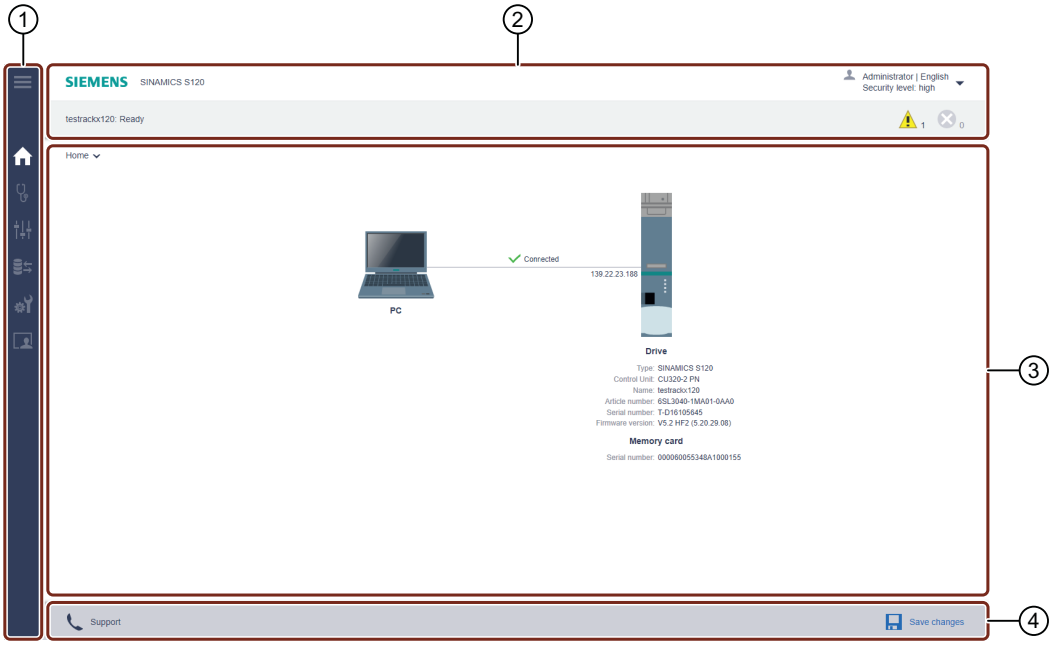
Saving settings retentively

Proceed as follows to save settings made retentively after automatic logout:

1. Log in to the web server.
2. Click "Save changes" .
   A corresponding dialog is displayed.
3. Click "Save".
   The settings are saved retentively.

A.2.1.10 Layout of the start page

After you have logged in, the web server will display the following start page:



1 Navigation bar

2 Status bar

- Top: Device designation, drop-down list for logout and language selection, display of the security level
- Bottom: Name of the converter (if entered), status of the converter, fault and warning messages

3 Main window (depending on navigation)

4 Action bar:

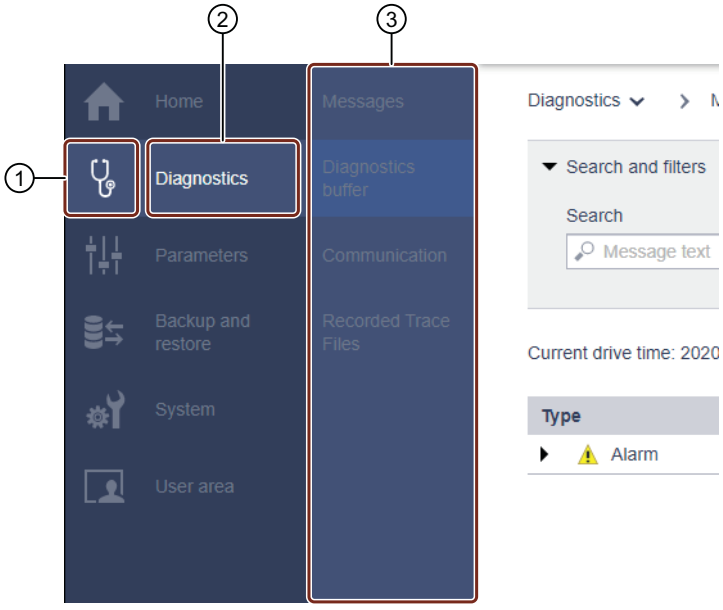
- Support information
- Save changes retentively (RAM to ROM)

Figure A-66 Structure of the web server

Navigation

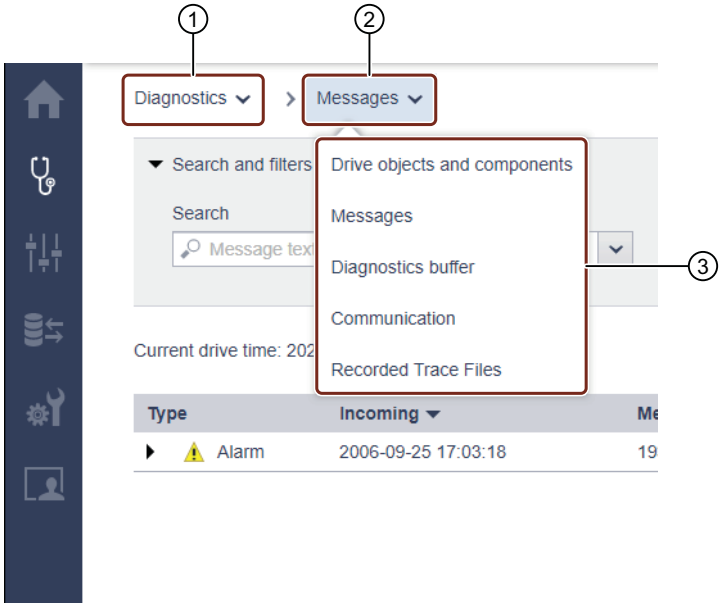
The web server provides the following options for navigating:

- Multi-level navigation bar:



① Main menu as icon
② Main menu in text format
③ Submenu(s) of the active main menu

- Via drop-down lists:



① Main menu in text format
② Submenu in text format
③ Submenu(s) of the active submenu

For navigation on mobile end devices, the screen forms can also be called in the active view of the web server via drop-down lists ① / ②.

Call support information

Overview

You call the support addresses for SINAMICS S120 via the action bar of the web server (see Chapter "Layout of the start page (Page 266)").

Procedure

Proceed as follows to call Support:

1. Click "Support" in the action bar of the web server.
   The following information is shown:

Figure A-67 Support addresses

   You can use the links to open or copy the desired support addresses.

2. Click "OK" to close the dialog.

Saving settings retentively

Overview

Changed settings are saved in the volatile memory of the converter, and retained when the web server is closed.

The settings are lost when the drive is switched off. Therefore, save the changes retentively on a regular basis (also known as "RAM to ROM"). You can save the changed settings and optimization results both for each individual commissioning step and after commissioning is complete.

Procedure

Proceed as follows to save changed settings retentively:

1. Click "Save changes" in the footer of the web server.
   A save dialog appears.
2. Click "Save".
   The settings are saved retentively.

A.2.1.11 Using SSL/TLS certificates for secure data transfer

Overview

You require a valid SSL/TLS certificate to establish a secure HTTPS connection between your commissioning device (PG/PC, tablet or smartphone) and the web server.

Establishing an HTTPS connection using a valid SSL/TLS certificate

The following options are available to establish a secure HTTPS connection using a valid SSL/TLS certificate:

- Use an SSL/TLS certificate from a certificate authority
- Use a user-defined SSL/TLS certificate
  When doing this, the user generates an SSL/TLS certificate using suitable software (e.g. OpenSSL). The user must ensure that the browser being used trusts the user-defined certificate and the HTTPS connection can be classified as secure.
  Additional information about calling a secure HTTPS connection when using a user-defined certificate is provided in Chapter "Using a self-created or purchased certificate (Page 271)".
- Using a self-signed certificate
  This certificate type is automatically generated when calling an HTTPS connection. The user must trust the self-signed certificate in order that a secure HTTPS connection can be established.
  Additional information about calling a secure HTTPS connection when using a self-signed certificate is provided in Chapter "Using a self-signed certificate (Page 273)".

Duration of validity

The certificates generated from the firmware files are valid until 01.01.2030. After expiration of the validity period, install new valid certificates on all the relevant drives.

Validating a server certificate

When calling an HTTPS connection to the web server, the validity of a server certificate is validated by the browser being used and the web server independent of the certificate type being used (e.g. a user-defined certificate). The following criteria are used for the validation:

Criterion	Browser	Web server
The server certificate originates from a certificate authority, whose private server key is contained in the Windows certificate store or in the certificate store of the browser being used in the list of trustworthy certification authorities.	X	–
The server certificate specifies the maximum validity period of the certificate.	X	X
The server certificate contains the currently valid IP addresses of service interface X127 and PROFINET interface X150. **Note** The server certificate can contain IP addresses set in the factory (e.g.: https://169.254.11.22 for service interface X127 at the converter) as well as user-defined IP addresses.	X	X

All criteria that are used as basis must be satisfied in order that a server certificate is validated. Server certificates that are not validated are classified as invalid.

Validation failed

When calling an HTTPS connection to the web server, if a self-signed certificate is not validated, the certificate is overwritten by a self-signed certificate that the converter automatically generates. This is applicable independent of the certificate type used.

Overwriting the previously used server certificate (e.g. a user-defined certificate) by a self-signed certificate can cause the web server to significantly slow down. To prevent this, depending on the browser being used, proceed as described in one of the following chapters:

- Internet Explorer 11 application (Page 274)
- Using Google Chrome and Microsoft edge (Page 281)
- Using Mozilla Firefox (Page 289)

Important notes

- Using an invalid server certificate:
  When calling an HTTPS connection to the web server, if you use a server certificate that is classified as invalid then this can significantly slow down the web server.
- Firmware version V5.2 SP3:
  If you upgrade your drive to the current firmware version V5.2 SP3, and the previously used server certificate is not validated when calling an HTTPS connection, the previously used server certificate is overwritten by a new self-signed certificate. This is applicable independent of the certificate type previously used.
  Validating a previously used server certificate can be unsuccessful for the following reasons, for example:
  - After the upgrade, the IP addresses of service interface X127 and/or PROFINET interface X150, included in the newly generated server certificate, do not match the IP addresses contained in the previously used server certificate.
  - The previously used server certificate only contains one IP address (e.g. IP address of the service interface X127).
    To validate a server certificate, the certificate must contain all the currently valid IP addresses of service interface X127 and PROFINET interface X150. Refer to the list of criteria above.

Using a self-created or purchased certificate

Overview

You can either generate your own SSL/TLS certificates for secure data transfer or purchase them from a certificate authority. You can find certificate authorities for purchasing certificates as well as software to generate certificates (e.g. OpenSSL) on the Internet.

As shown in the following example, a valid SSL/TLS certificate comprises a server certificate and a private server key. The server certificate and the private key must be individualized for the relevant IP address.

- Server certificate: <IP addr>.TLS.crt Example: 192.168.2.90.TLS.crt
- Private server key: <IP addr>.TLS.key Example: 192.168.2.90.TLS.key

Requirements

- You have connected your commissioning device to service interface X127 or PROFINET interface X150.
- You have administrator rights on your commissioning device.
- You have a user-defined or purchased SSL/TLS certificate comprising server certificate (*.crt) and private server key (*.key). Certificate files (*.crt and *.key) are saved in your commissioning device in a folder that only you can access.

Copying the certificate files to a Siemens memory card

Proceed as follows to copy a user-defined or purchased SSL/TLS certificate to the Siemens memory card of your SINAMICS S120 drive:

1. Switch off your drive.
2. Remove the Siemens memory card from the drive.
3. Copy the certificate files (*.crt and *.key) into the following directory on the Siemens memory card:
   – OEM\SINAMICS\HMICFG\CERTSTORES\SERVERCERTS
4. Rename the server certificate as "SINAMICS.crt".
5. Rename the private server key as "SINAMICS.key".
6. Insert the Siemens memory card into your drive.
7. Switch on your drive.
   The drive powers up.
8. Wait until the drive has finished ramping up.
9. Proceed as described in the following section.

Establishing a secure HTTPS connection

Proceed as follows to establish a secure HTTPS connection between the browser and the web server:

1. Open the browser.
2. Call the web server using the IP address of your drive (e.g.: https://169.254.11.22 for service interface X127 at the converter).
   The login page of the web server opens.
   Generally, a secure connection is indicated using a lock symbol in the browser address line.

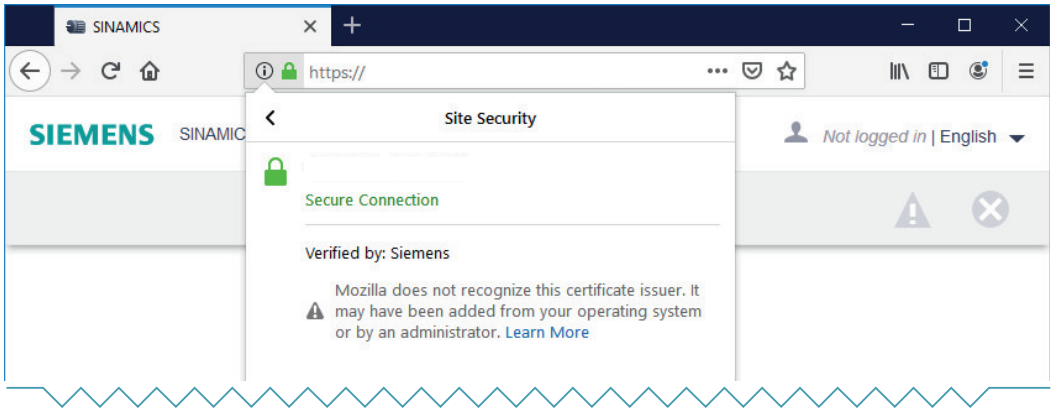


Figure A-68 Example: Mozilla Firefox

By copying the certificate files (*.crt and *.key) to the Siemens memory card of your SINAMICS drive, the user-defined or purchased server certificate is validated, and the HTTPS connection is classified as being secure.

Validation failed

If the user-defined or purchased server certificate is not validated, as an alternative you can use a self-signed certificate.

Additional information for using self-signed certificates is provided in Chapter "Using a self-signed certificate (Page 273)".

Using a self-signed certificate

Overview

The converter automatically generates a server certificate when first establishing an HTTPS connection to the web server. The certificate files required (*.crt and *key) are included in the firmware files of the converter.

In this case, the self-signed certificate is individualized for the IP address of the interface, via which communication is established (e.g.: https://169.254.11.22 for service interface X127 at the converter).

Security warning with non-secure HTTPS connection

The usual Internet browsers do not validate self-signed certificates. As a consequence, the browser classifies these certificates as invalid, and when calling an HTTPS connection first issues a security warning.

For the browser to trust a self-signed certificate, the self-signed certificate must first be exported from the browser and then installed or imported into the certificate store of the Windows system.

A secure HTTPS connection can be established once the self-signed certificate has been successfully installed or has been imported into the certificate store of the Window system.

Managing certificates in common browsers

The essential features and special issues relating to the following browsers in conjunction with certificate management in the Window system are listed in the following table:

Browser	Version	Engine	Certificate management
Google Chrome	80.0.3987.122 [64 bit]	Chromium	The browser only accesses certificates that are saved in the certificate store of the Windows system. A self-signed certificate cannot be directly installed from the browser.
Microsoft Edge	81.0.416.72 [64 bit]		
Mozilla Firefox	68.8.0 ESR [32 bit]	Gecko	Data relating to Google Chrome and Microsoft Edge are applicable. Mozilla Firefox also has its own certificate management integrated in the browser.
Internet Explorer 11	11.1425.17134.0	Trident	A self-signed certificate can be directly installed from the browser. The certificate is saved in the certificate store of the Windows system.

Restrictions

The descriptions in this chapter refer exclusively to the browser versions listed above. Browser response can deviate depending on the browser version being used. The display examples contained in this chapter may differ from the displays in your browser or commissioning device.

Important notes

- Using a self-signed certificate as subsequently described does not represent the most secure form of data transfer via an HTTPS connection. Only use the self-signed certificate in secure networks (e.g. PROFINET below a PLC) or for direct point-to-point connections to the service interface X127 or PROFINET interface X150.

Internet Explorer 11 application

Overview

Internet Explorer 11 uses the "Trident" browser engine and accesses the Windows certificate store. Using Internet Explorer 11 self-signed certificates can be installed in the Window certificate store directly from the browser.

It is crucial that the subsequently described steps are complied with to establish a secure HTTPS connection between the browser and the web server.

Important notes

- Certificates, which are installed in the Windows certificate store using Internet Explorer 11 and are classified as valid, are also available for other browsers (e.g. Chrome, Edge, Firefox). This applies to all certificate types.

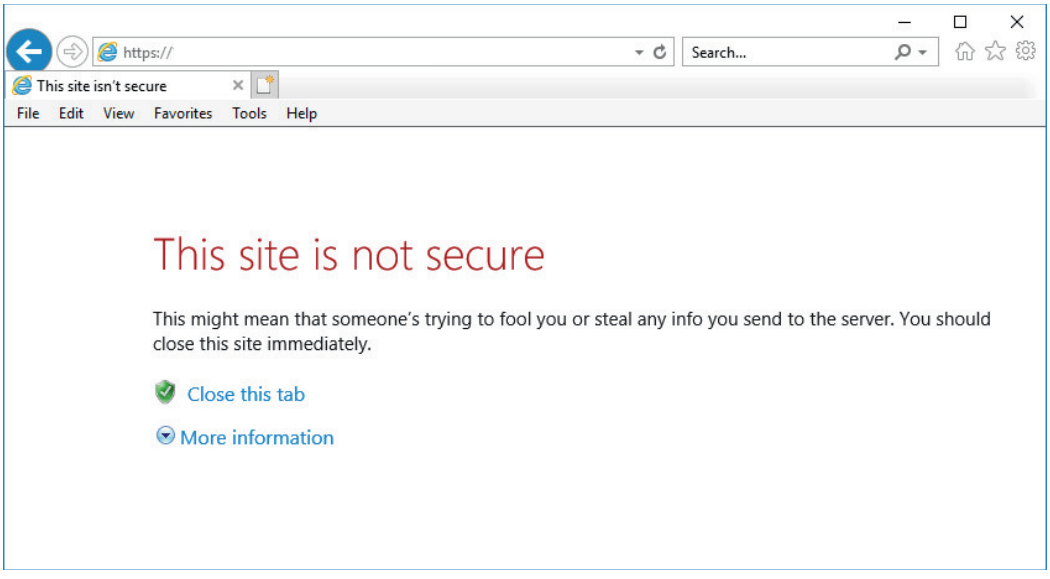
Requirements

- You have connected your commissioning device to service interface X127 or PROFINET interface X150.
- You have administrator rights on your commissioning device.

Calling the web server via an HTTPS connection

Proceed as follows to establish an HTTPS connection between the browser and the web server:

1. Open the browser.
2. Call the web server using the IP address of your drive (e.g.: https://169.254.11.22 for service interface X127 at the converter).
   When establishing the HTTPS connection, the converter automatically generates a server certificate. The self-signed certificate is individualized for the IP address of the interface being used.
   The browser classifies the certificate as being invalid, and responds with a security warning.

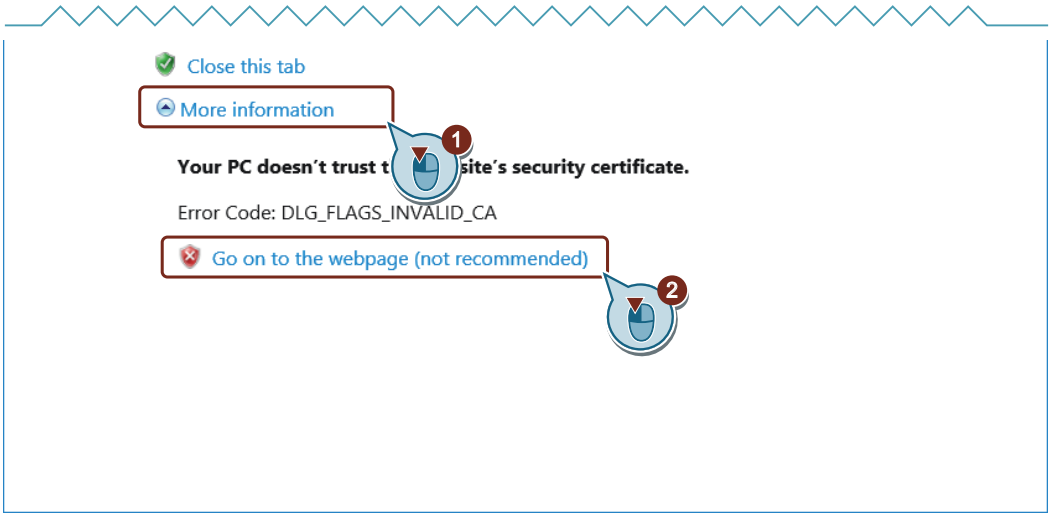


3. Proceed as described in the following section.

Installing a certificate

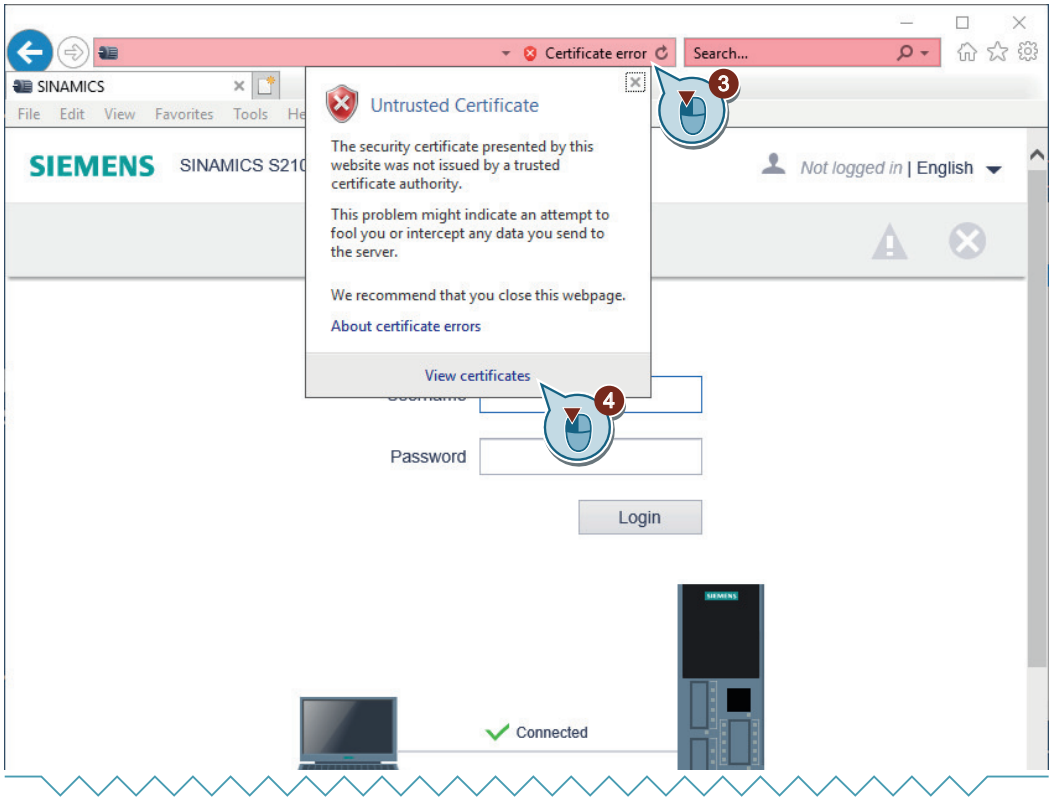
Proceed as follows to install the self-signed certificate:

1. In the the opened webpage, click on option "More information" ①.



2. Click on "Go on to the web page (not recommended)" ②.
   The login page of the web server opens.
   Status "Certificate error" is displayed in the browser address line.

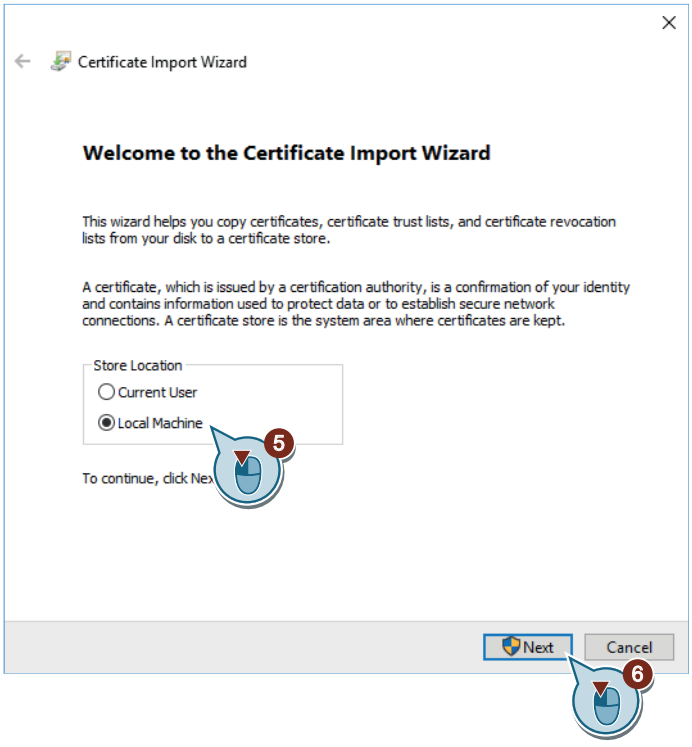
3. In the browser address line, click on status display "Certificate error" ③.



A corresponding dialog is displayed.

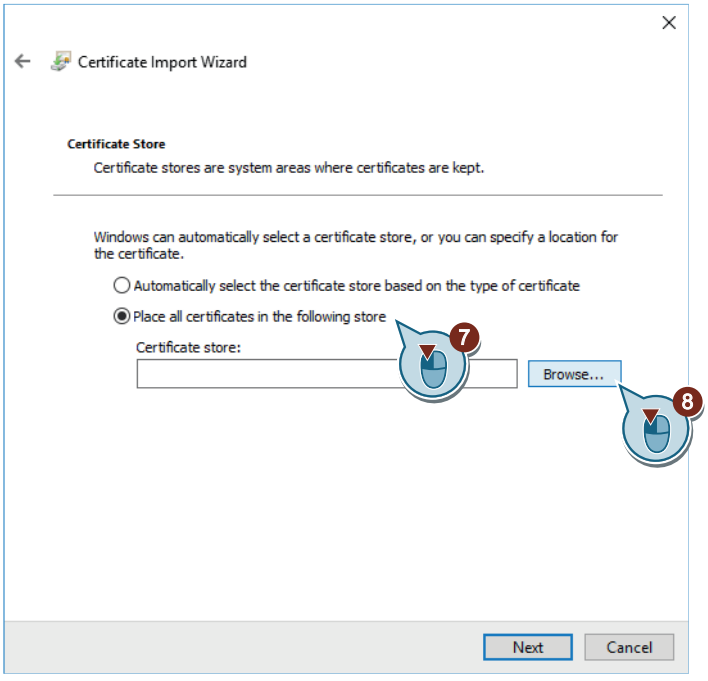
4. Click on "Display certificate" ④.
   Dialog "certificate" opens.
5. Under tab "General", click on "Install certificate...".
   The "Certificate Export Wizard" opens.

6. On the wizard welcome page, select option "Local computer" ⑤.

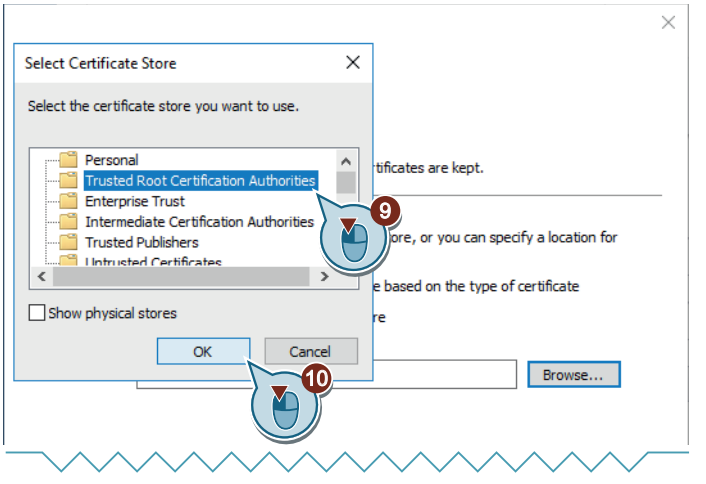


7. To continue the operation, click on "Next" ⑥.
   The "User Account Control" dialog opens.
8. Acknowledge the confirmation prompt with "Yes".
   The dialog to select the certificate store opens.

9. Select option "Place all certificates in the following store" ⑦.



10. Click on "Browse..." ⑧.
    A corresponding dialog opens.
11. Select the certificate store "Trusted Root Certification Authorities" ⑨.



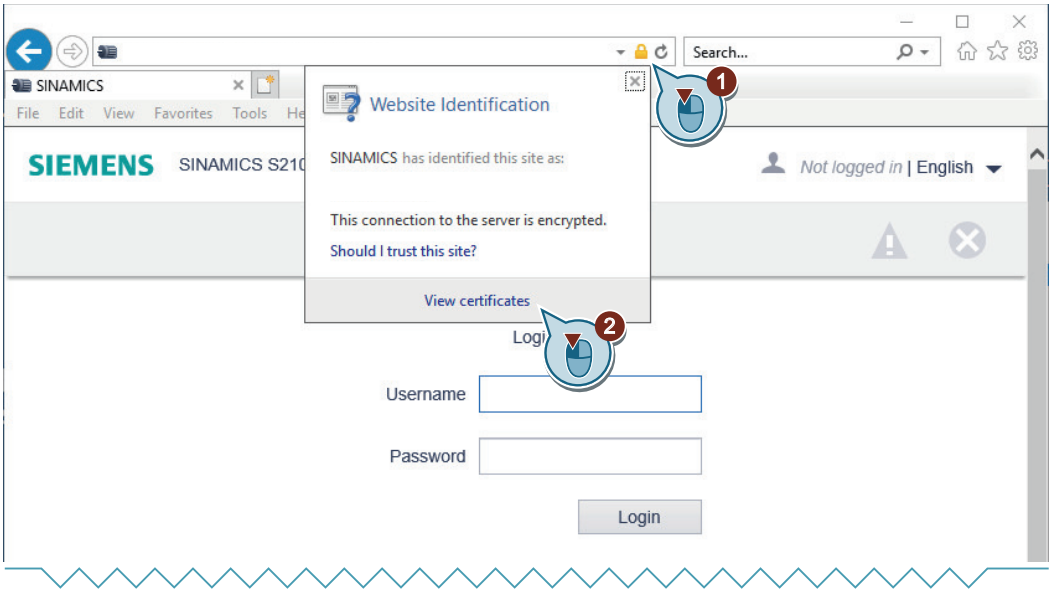
12. Click "OK" ⑩ to confirm the selection.
13. To continue the operation, click on "Next".
    An overview of the settings made is displayed for you to check.
14. Click "Finish" to apply the settings.
    The Wizard reports that the export has been completed successfully.
15. Confirm the procedure with "OK".
    The Wizard closes.

16. Close dialog "Certificate".
17. Close the browser.
18. Proceed as described in the following section.

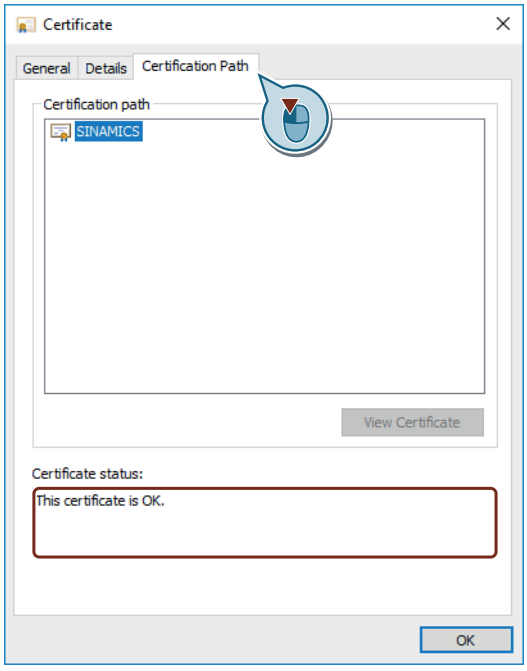
Establishing a secure HTTPS connection

Proceed as follows to establish a secure HTTPS connection between the browser and the web server:

1. Open the browser.
2. Call the web server using the IP address of your drive (e.g.: https://169.254.11.22 for service interface X127 at the converter).
   The login page of the web server opens.
   A secure connection is indicated using a lock symbol in the browser address line.
3. Click on the lock symbol ① to check the certification status .



4. Click on "View certificates".
   Dialog "certificate" opens.
5. Click on tab "Certification Path".
   The certification status is displayed in the lower part of the window.



The self-signed certificate is validated, and the HTTPS connection is classified as secure by installing the automatically generated server certificate in the Windows certificate store.

Using Google Chrome and Microsoft edge

Overview

Google Chrome and Microsoft Edge use the "Chromium" browser engine, and when checking certificates, access the Windows certificate store. This applies to all browsers that use "Chromium" as browser engine.

To keep it simple, only screen examples from Google Chrome are subsequently shown. The term "Browser" refers to both Google Chrome and Microsoft Edge.

It is crucial that the subsequently described steps are complied with to establish a secure HTTPS connection between the browser and the web server.

Important notes

- Certificates that are installed in the Windows certificate store using Internet Explorer 11 and are classified as valid are also available for other browsers (e.g. Chrome, Edge, Firefox). This applies to all certificate types.
  If you have already installed the self-signed certificate using Internet Explorer 11, then you can skip the steps described below and go directly to section "Establishing a secure HTTPS connection". Otherwise, proceed as described below.

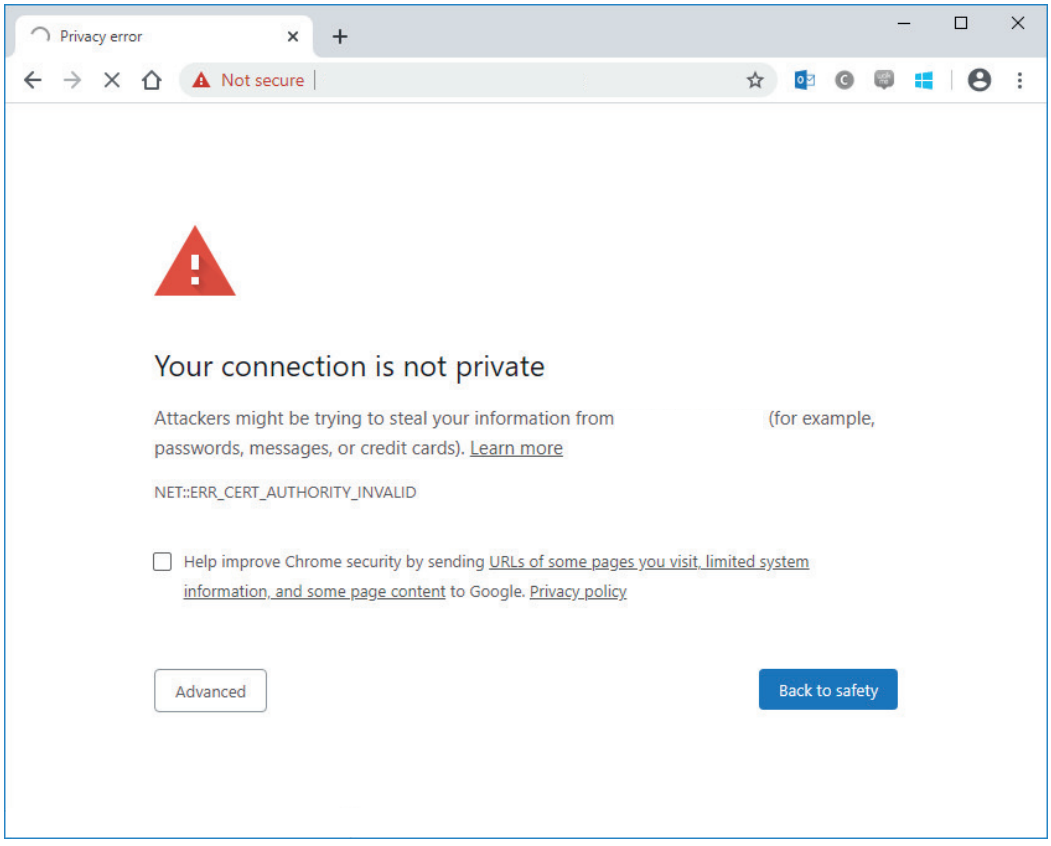
Requirements

- You have connected your commissioning device to service interface X127 or PROFINET interface X150.
- You have administrator rights on your commissioning device.

Calling the web server via an HTTPS connection

Proceed as follows to establish an HTTPS connection between the browser and the web server:

1. Open the browser.
2. Call the web server using the IP address of your drive (e.g.: https://169.254.11.22 for service interface X127 at the converter).
   When establishing the HTTPS connection, the converter automatically generates a server certificate. The self-signed certificate is individualized for the IP address of the interface being used.
   The browser classifies the certificate as being invalid, and responds with a security warning.

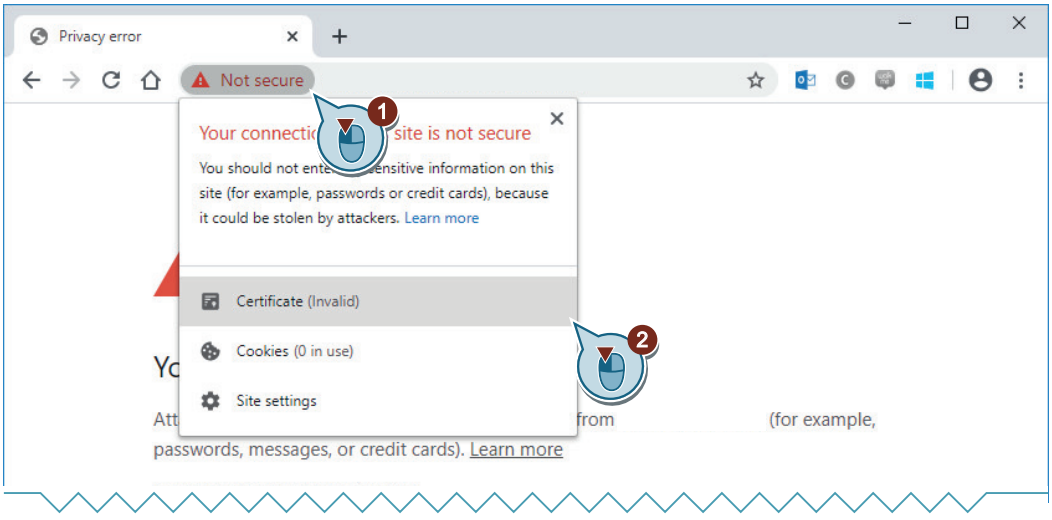


3. Proceed as described in the following section.

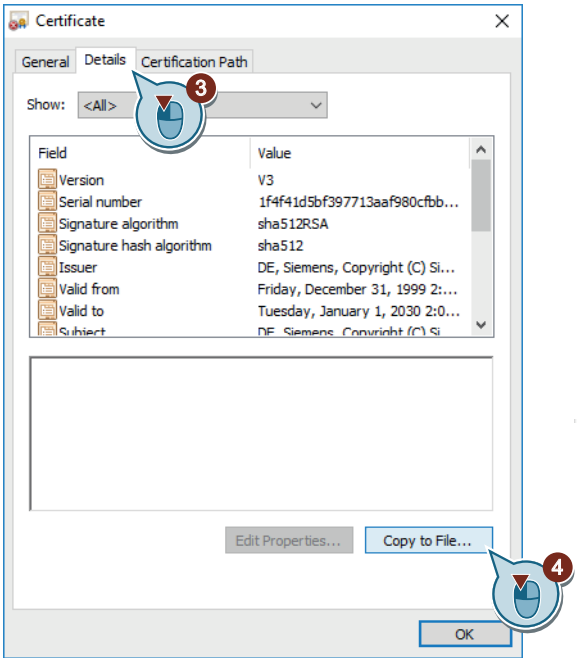
Exporting a certificate

Proceed as follows to export the generated certificate:

1. In the browser address line, click on status display "Not secure" ①.
   A corresponding dialog opens.

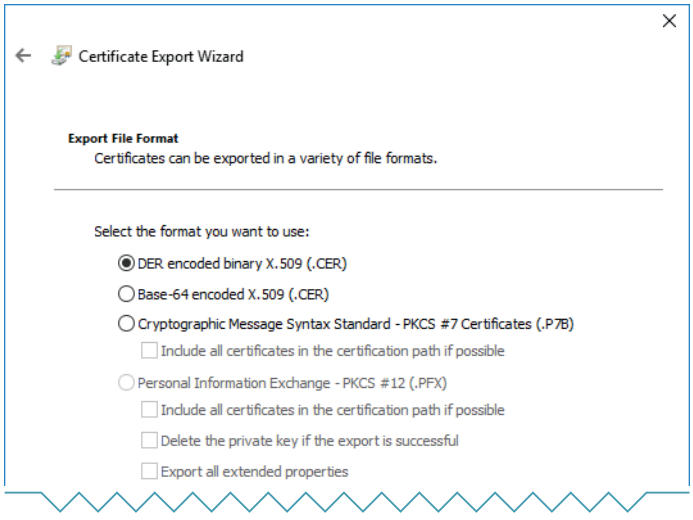


2. Click on "Certificate (invalid)" ②.
   Dialog "certificate" opens.
3. Click the "Details" tab ③.

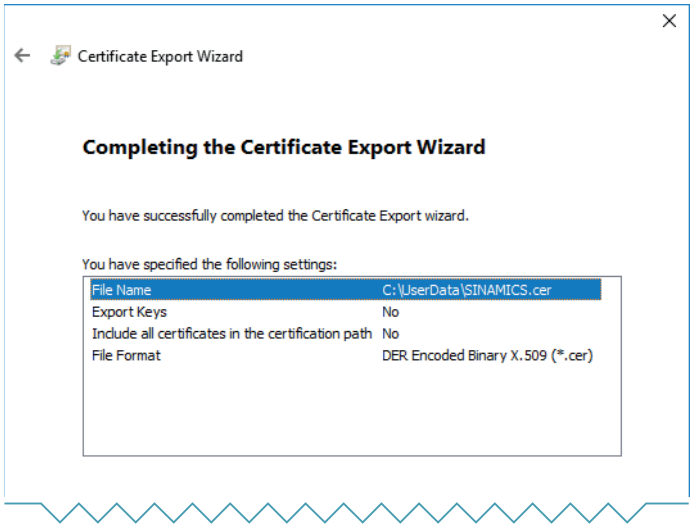


4. To export the certificate, click on "Copy to File..." ④.
   The "Certificate Export Wizard" opens.

5. On the Wizard welcome page, click on "Next".
   The dialog for selecting the export format opens.
   In the default setting, format "DER-coded-binary X.509 (.CER)" is selected.



6. To continue the operation, click on "Next".
   The dialog for selecting the storage location opens.
7. Click on "Browse...".
   The file explorer opens.
8. Navigate to the desired storage location.
9. Assign a descriptive name to the certificate and then click on "Save".
   The file explorer closes.
10. To continue the operation, click on "Next".
    An overview of the settings made is displayed for you to check.



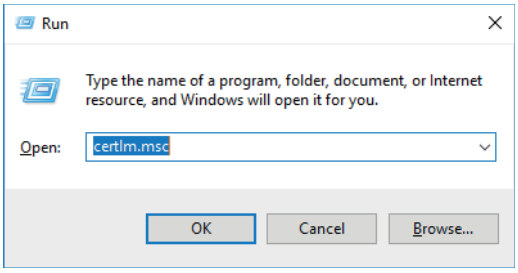
11. Click "Finish" to apply the settings.
    The Wizard reports that the export has been completed successfully.

12. Confirm the procedure with "OK".
    The Wizard closes.
13. Close dialog "Certificate".
14. Close the browser.
15. Proceed as described in the following section.

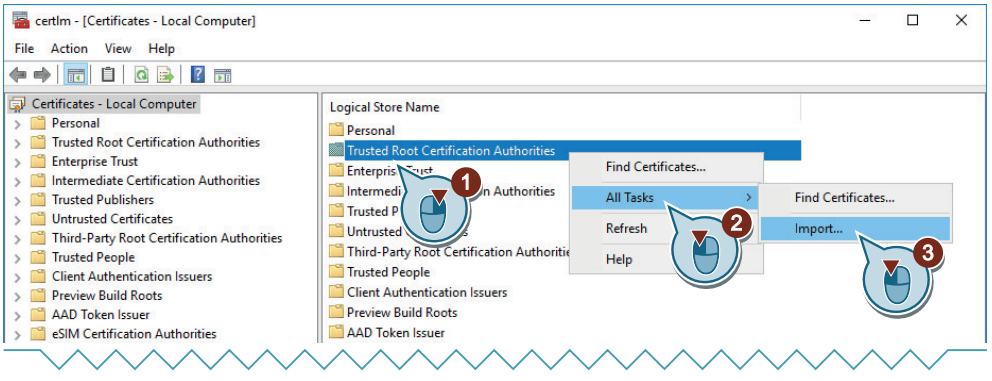
Importing a certificate

Proceed as follows to import the certificate that was exported to the Windows certificate store:

1. Press the keys + R at the same time.
   The command line input opens.
2. Enter the command "certlm.msc" and click "OK".

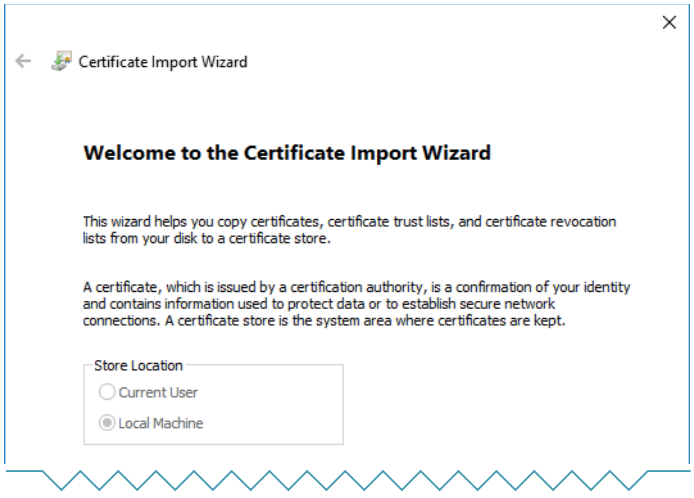


   The "User Account Control" dialog opens.
3. Confirm the prompt in the "User Account Control" dialog with "Yes".
   The certificate store opens.
4. Right-click the "Trusted Root Certification Authorities" folder ①.

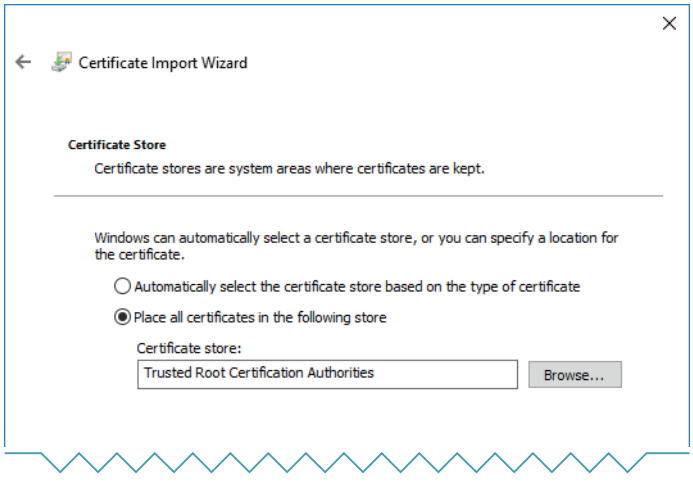


   The possible actions are displayed.
5. Click "All Tasks" ②.
   The tasks are displayed.

6. Click "Import" ③.
   The "Certificate Import Wizard" opens.
   "Local Machine" is preset as storage location.



7. To continue the operation, click on "Next".
   The dialog for specifying the certificate to be imported opens.
8. Click "Browse...".
   The file explorer opens.
9. Go to the storage location of the exported certificate.
10. Click on the certificate to be imported.
    The path is displayed in the "File name" input field.
11. To continue the operation, click on "Next".
    The dialog for selecting the certificate store opens.
    The "Trusted Root Certification Authorities" certificate store is already set.



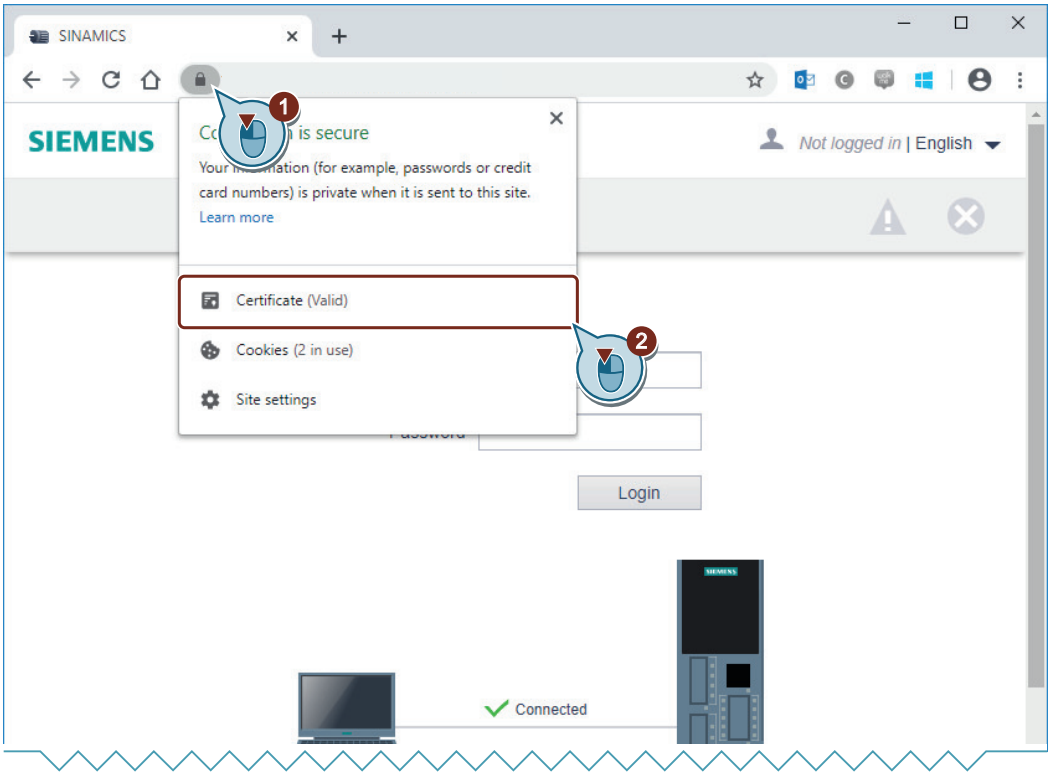
12. Confirm the settings with "Next".
    An overview of the settings made is displayed for you to check.

13. Click "Finish" to apply the settings.
    The Wizard reports that the import has been successfully completed.
14. Confirm the procedure with "OK".
    The Wizard closes.
15. Close the certificate store.
16. Proceed as described in the following section.

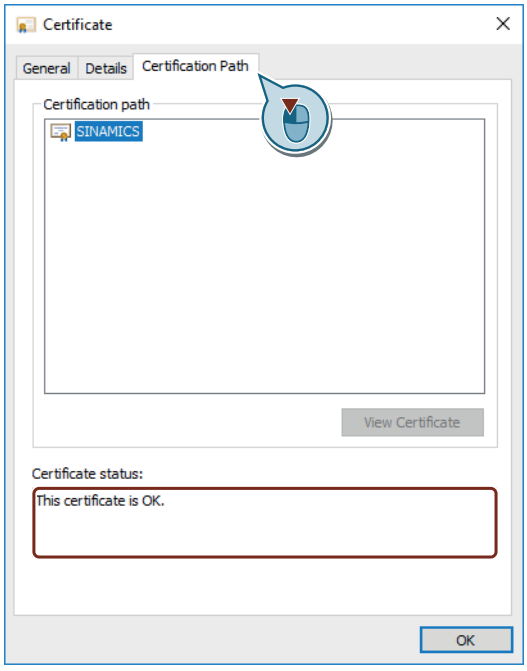
Establishing a secure HTTPS connection

Proceed as follows to establish a secure HTTPS connection between the browser and the web server:

1. Open the browser.
2. Call the web server using the IP address of your drive (e.g.: https://169.254.11.22 for service interface X127 at the converter).
   The login page of the web server opens.
   A secure connection is indicated using a lock symbol in the browser address line.
3. Click on the lock symbol ① in the browser address line to check the certification status.



4. Click on "Certificate (valid)" ②.
   Dialog "certificate" opens.
5. Click on tab "Certification Path".
   The certification status is displayed in the lower part of the window.



The self-signed certificate is validated, and the HTTPS connection is classified as secure by installing the self-signed certificate in the Windows certificate store.

Using Mozilla Firefox

Overview

Mozilla Firefox uses browser engine "Gecko", and in addition to its own browser certificate management, it also accesses the Windows certificate store.

It is crucial that the subsequently described steps are complied with to establish a secure HTTPS connection between the browser and the web server.

Important notes

- Certificates that are installed in the Windows certificate store using Internet Explorer 11 and are classified as valid are also available for other browsers (e.g. Chrome, Edge, Firefox). This applies to all certificate types.
  If you have already installed the self-signed certificate using Internet Explorer 11, then you can skip the steps described below and go directly to section "Establishing a secure HTTPS connection". Otherwise, proceed as described below.

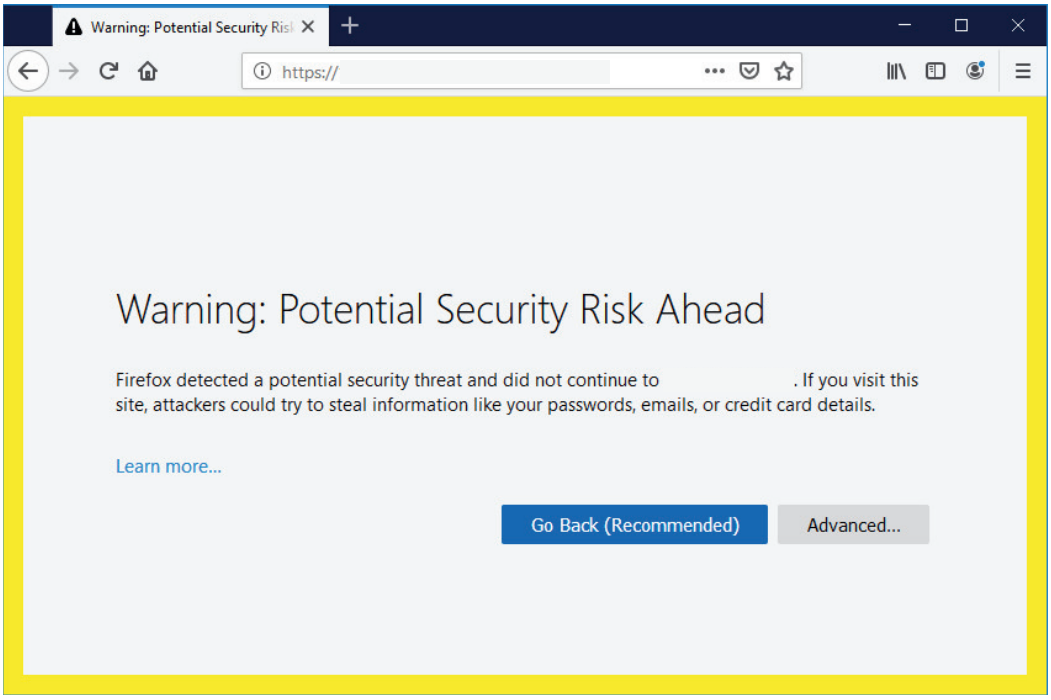
Requirements

- You have connected your commissioning device to service interface X127 or PROFINET interface X150.
- You have administrator rights on your commissioning device.

Calling the web server via an HTTPS connection

Proceed as follows to establish an HTTPS connection between the browser and the web server:

1. Open the browser.
2. Call the web server using the IP address of your drive (e.g.: https://169.254.11.22 for service interface X127 at the converter).
   When establishing the HTTPS connection, the converter automatically generates a server certificate. The self-signed certificate is individualized for the IP address of the interface being used.
   The browser classifies the certificate as being invalid, and responds with a security warning.

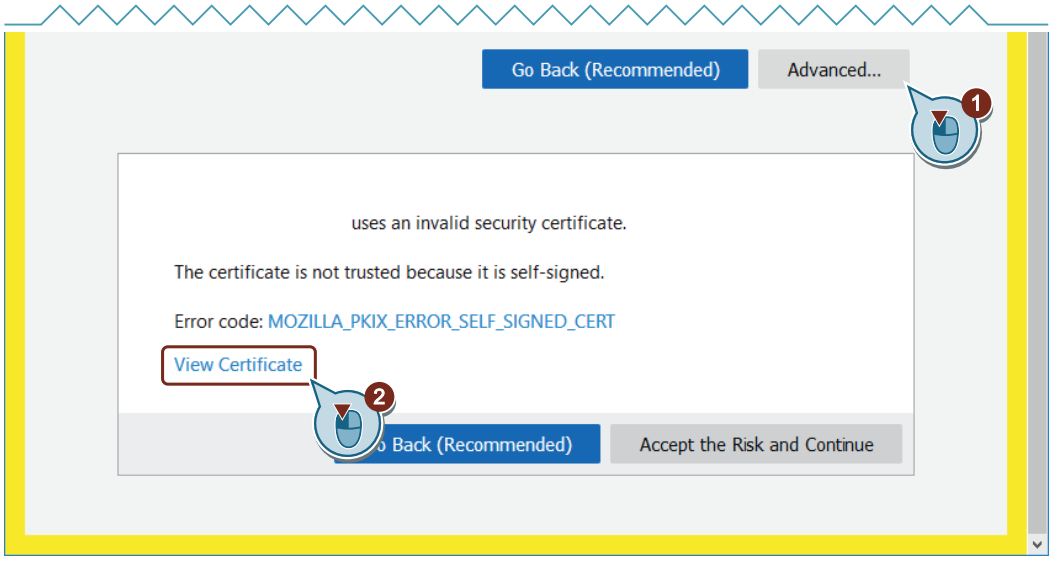


3. Proceed as described in the following section.

Exporting a certificate

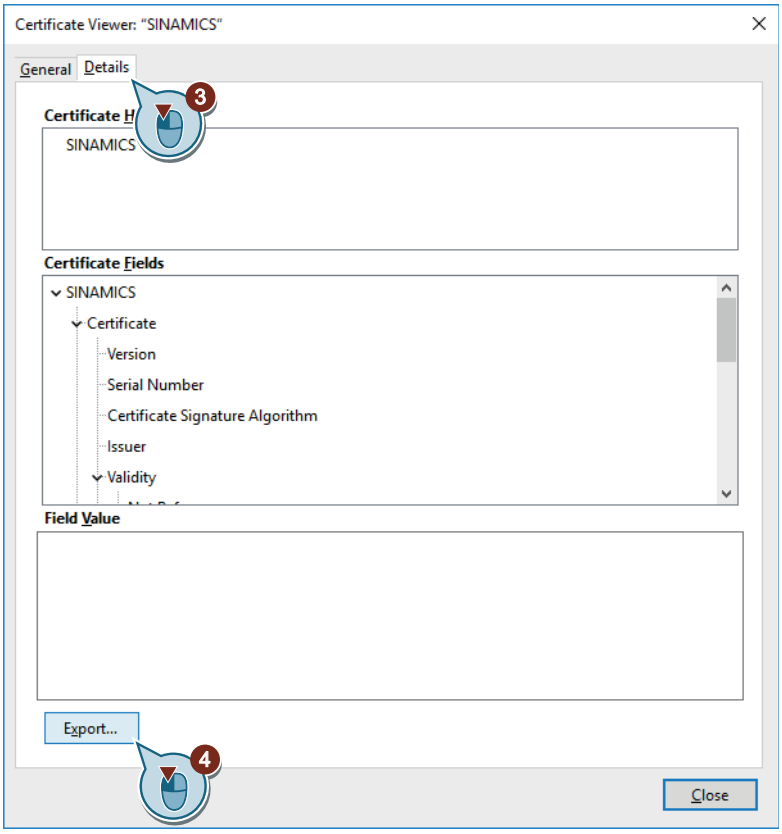
Proceed as follows to export the generated certificate:

1. In the open page, click on "Advanced" ①.
   A field with additional details and options is displayed.



2. Click on "View Certificate" ②.
   Dialog "Certificate view: SINAMICS" opens.

3. Click the "Details" tab ③.

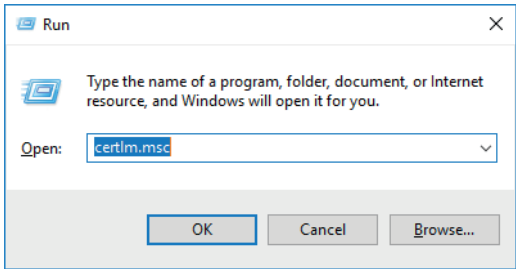


4. To export the certificate, click on "Export..." ④.
   The file explorer opens.
5. Navigate to the desired storage location.
6. Assign a descriptive name to the certificate and then click on "Save".
   The file explorer closes.
7. Close the dialog.
8. Close the browser.
9. Proceed as described in the following section.

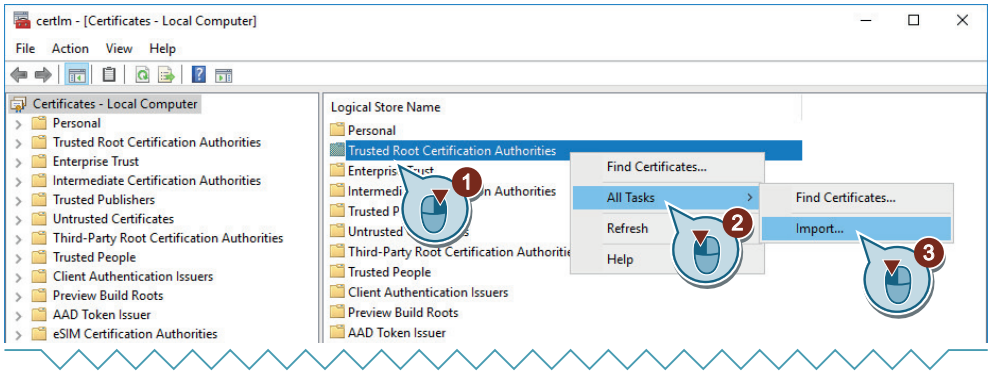
Importing a certificate

Proceed as follows to import the certificate that was exported to the Windows certificate store:

1. Press the keys + at the same time.
   The command line input opens.
2. Enter the command "certlm.msc" and click "OK".

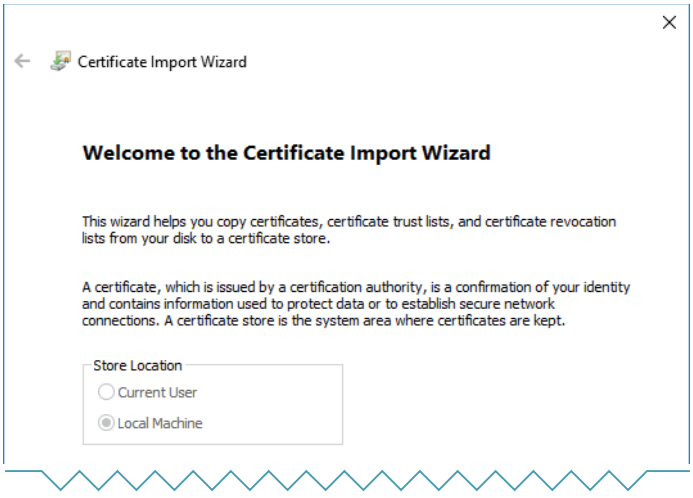


   The "User Account Control" dialog opens.
3. Confirm the prompt in the "User Account Control" dialog with "Yes".
   The certificate store opens.
4. Right-click the "Trusted Root Certification Authorities" folder ①.

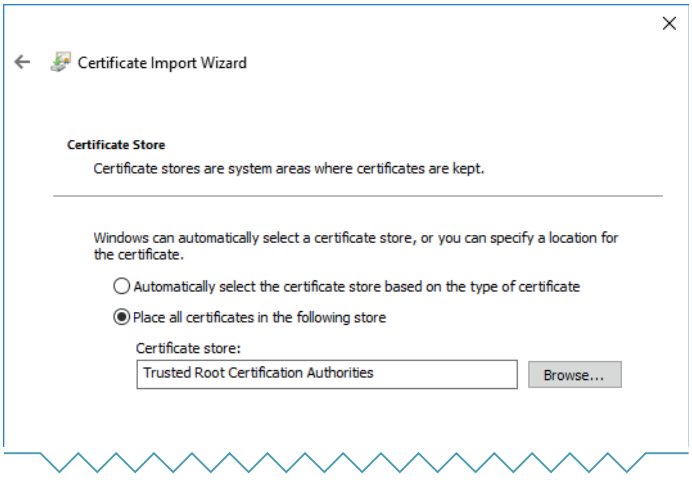


   The possible actions are displayed.
5. Click "All Tasks" ②.
   The tasks are displayed.

6. Click "Import" ③.
   The "Certificate Import Wizard" opens.
   "Local Machine" is preset as storage location.



7. To continue the operation, click on "Next".
   The dialog for specifying the certificate to be imported opens.
8. Click "Browse...".
   The file explorer opens.
9. Go to the storage location of the exported certificate.
10. Click on the certificate to be imported.
    The path is displayed in the "File name" input field.
11. To continue the operation, click on "Next".
    The dialog for selecting the certificate store opens.
    The "Trusted Root Certification Authorities" certificate store is already set.



12. Confirm the settings with "Next".
    An overview of the settings made is displayed for you to check.

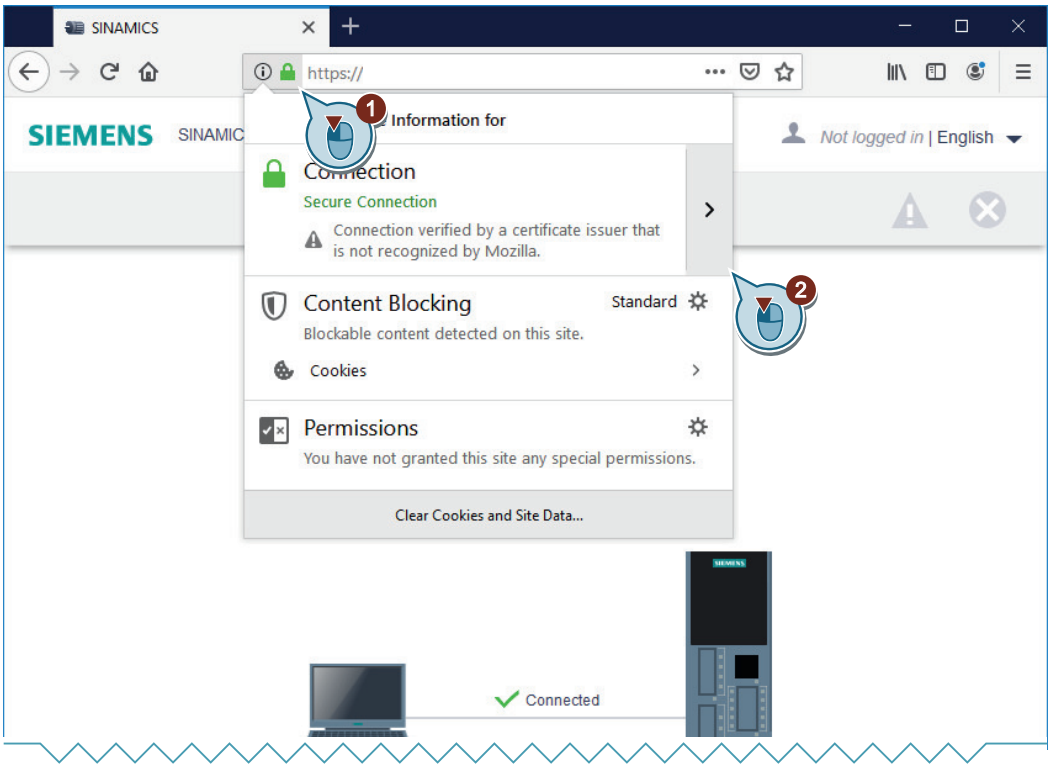
13. Click "Finish" to apply the settings.
    The Wizard reports that the import has been successfully completed.
14. Confirm the procedure with "OK".
    The Wizard closes.
15. Close the certificate store.
16. Proceed as described in the following section.

Establishing a secure HTTPS connection

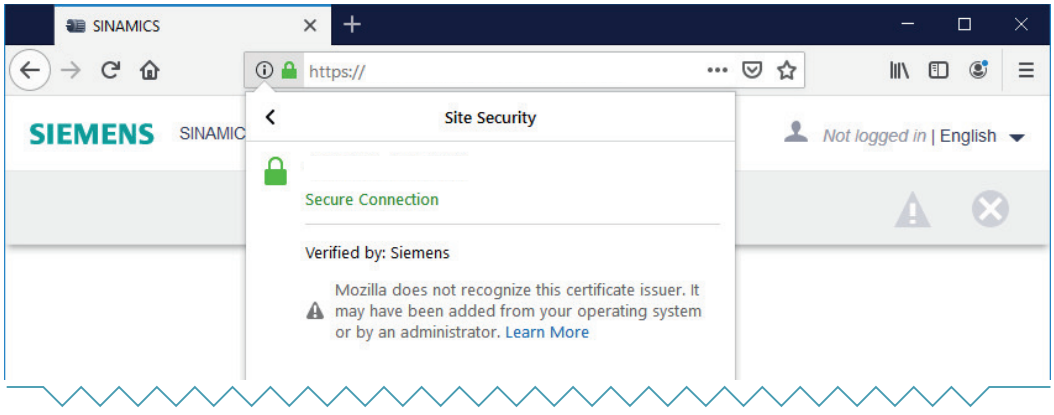
Proceed as follows to establish a secure HTTPS connection between the browser and the web server:

1. Open the browser.
2. Call the web server using the IP address of your drive (e.g.: https://169.254.11.22 for service interface X127 at the converter).
   The login page of the web server opens.
   A secure connection is indicated using a lock symbol in the browser address line.

3. Click on the lock symbol ① in the browser address line to check the status of the HTTPS connection.



4. To obtain additional details, click on button ② next to the displayed status message.



The self-signed certificate is validated, and the HTTPS connection is classified as secure by installing the self-signed certificate in the Windows certificate store.

A.2.2 Diagnostic functions

A.2.2.1 "Drive objects and components" display area

In the "Drive objects and components" display area, you can view information on the drive objects and components as well as on DRIVE-CLiQ wiring errors.

View drive objects

To display of drive objects for your drive, proceed as follows:

Procedure

1. Click in the "Drive objects and components" display area on the "Drive objects" tab.
   Then, the information and messages regarding the drive objects are displayed in a list.

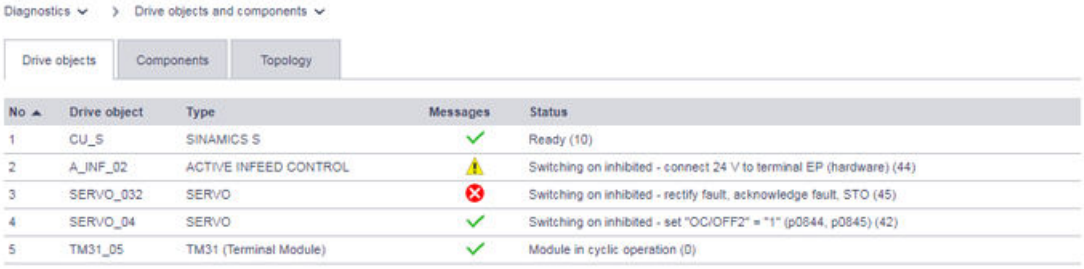


Figure A-69 Example: Drive objects display area

2. If needed, you can re-sort the individual columns by clicking on the corresponding column head (e.g. Type).
   You can view the entries in ascending ▲ or descending ▼ order.

Note

Re-sorting the entries in a list affects only the list currently being shown. Re-sorting has no effect on other lists.

Displaying and identifying components

In order to view the components of your drive, proceed as follows:

Procedure

1. Click in the “Drive objects and components” display area on the “Components” tab.
   Then, the information and messages regarding the components are displayed in a list.

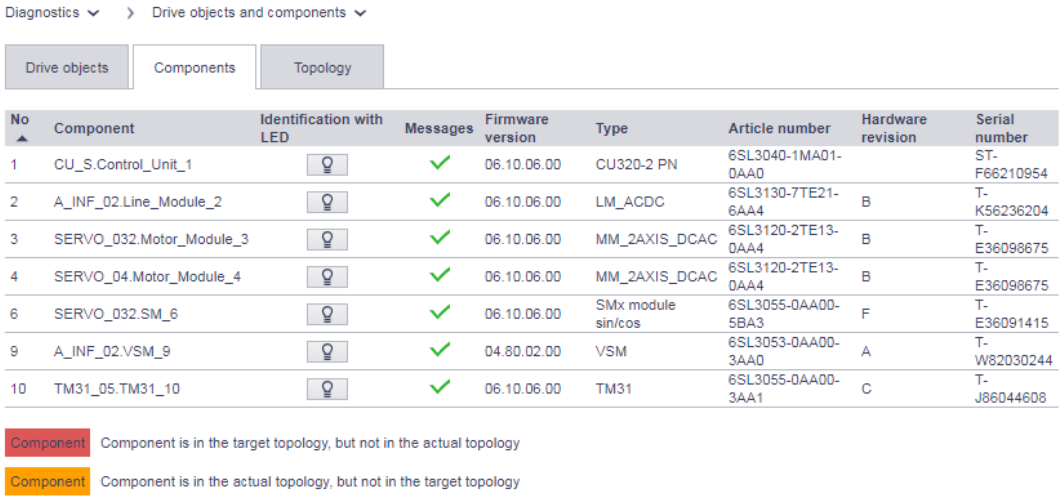


Figure A-70 Example: “Components” display area

2. In order to carry out an LED flash test for individual components, click on in the corresponding line.
   The ready LED on the corresponding component then begins to flash.
3. If needed, you can re-sort the individual columns by clicking on the corresponding column head (e.g. Type).
   You can view the entries in ascending ▲ or descending ▼ order.

Note

Re-sorting the entries in a list affects only the list currently being shown. Re-sorting has no effect on other lists.

A red or orange marking indicates a DRIVE-CLiQ wiring error on a component. Switch to the “Topology” tab in order to view further information.

Displaying DRIVE-CLiQ wiring errors

In order to view existing DRIVE-CLiQ wiring errors and diagnostic information about the individual components of your drive, proceed as follows:

Procedure

1. Click in the "Drive objects and components" display area on the "Topology" tab.
   Then the diagnostic information about the components is shown in a list. Using the information in the "Separate Port," "Uplink to Port" and "Uplink to number" columns, you can diagnose wiring errors on the individual components.

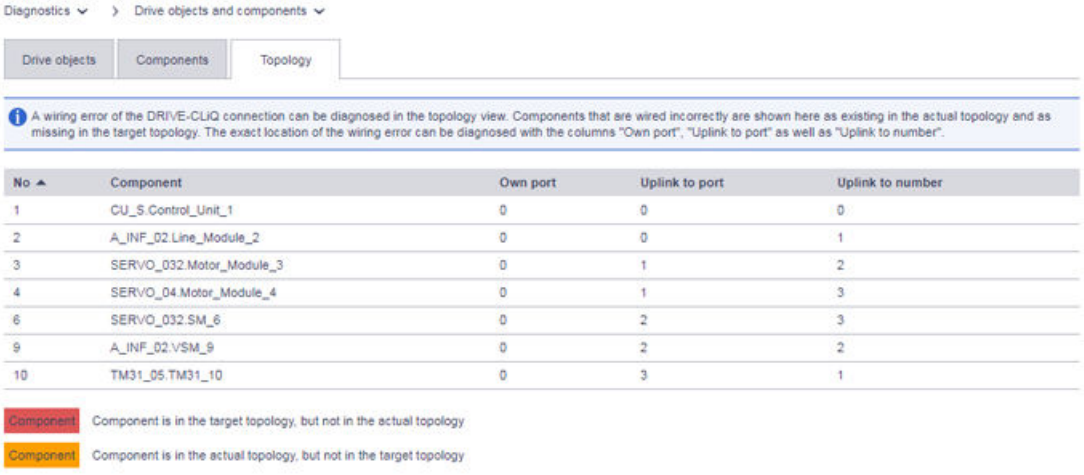


Figure A-71 Example: Topology display area

2. If needed, you can re-sort the individual columns by clicking on the corresponding column head (e.g. Type).
   You can view the entries in ascending ▲ or descending ▼ order.

Note

Re-sorting the entries in a list affects only the list currently being shown. Re-sorting has no effect on other lists.

A.2.2.2 "Alarms" display area

In the "Messages" display area, you can view the messages regarding the drive objects. In addition to this, the display area provides you with the following options:

- Filtering according to message text.
- Selecting messages regarding specific drive objects.
- Filtering messages according to date.
- In order to compare current and past states to each other, you can activate the "View message history" option.
- Filtering messages according to the respective message type.
- Acknowledging messages.
- In order to evaluate messages in greater detail, you can view additional details for the messages.

The following description addresses exclusively the fundamental configuration and operation options in the display area "Messages."

Meaning of the symbols

The symbols indicate the following states of individual drive objects:

Alarm
Fault
Acknowledged fault

Viewing messages and additional information

In order to call up the list of messages, proceed as follows:

1. Select "Diagnostics > Messages" in the navigation.
   OR
2. Click in the header of the web server on the or symbols.

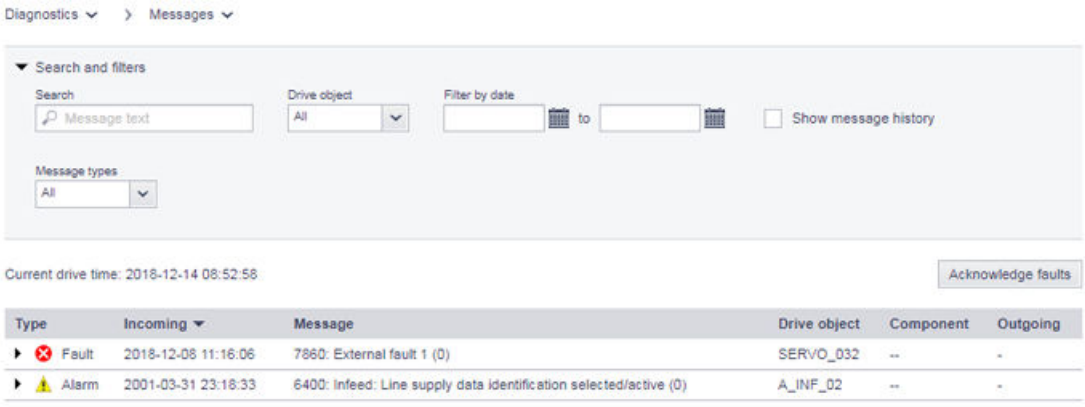


Figure A-72 Example: Message list

3. In order to view additional details on individual messages, click anywhere in the corresponding line.
   Then, under the corresponding message, an additional line with details and instructions is shown. If additional information has been stored, it appears in the line under the corresponding messages. Otherwise, the line is shown without content.

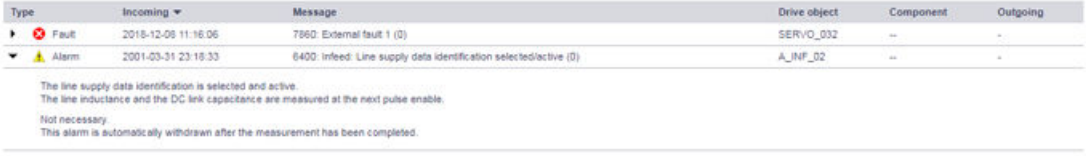


Figure A-73 Example: Further information

4. If needed, you can re-sort the individual columns by clicking on the corresponding column head (e.g. Type).
   You can view the entries in ascending ▲ or descending ▼ order.

Note

Re-sorting the entries in a list affects only the list currently being shown. Re-sorting has no effect on other lists.

Filtering messages

You can set filters in the message list and therefore limit the display of the messages. You can configure the filter settings using the error bar above the message list. All filters are linked by a logical conjunction (AND).

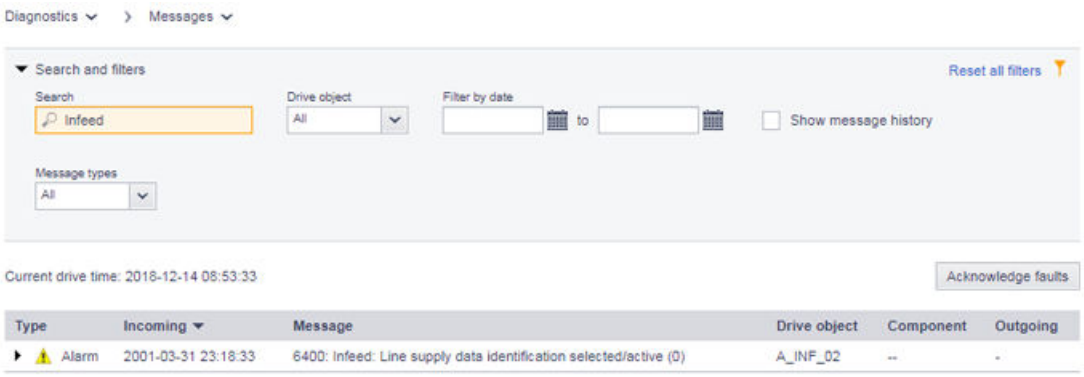


Figure A-74 Example: Filtering messages

Setting filters

Proceed as follows to set the filters in the “Search and filter” filter bar.

Note

Collapsing the filter bar

The filter bar is opened per default. To close the filter bar, click anywhere in the header of the “Search and filter” bar.

Procedure

1. In the "Search" field, enter a search term (any number of characters) for which you want to search in the message list.
   The search results are displayed in the message list.

   Note

   The search term is applied to the "Message" column in the message list.

2. If necessary, select a drive object and, in the “Filter by date” fields, determine a date range for which you want to display messages.
   After each setting is configured, the search results in the message list are narrowed down further. The filters can be set in any order.

Resetting filters

As long as you are logged in to the web server and the filter settings have not changed, the message list is always displayed with the last filter settings. In order to reset all filter settings in the message list, proceed as follows:

Procedure

1. Click "Reset all filters" at the top right in the filter bar.
   You have now re-set all configured filters. The message list then displays the unfiltered view of the messages again.

Acknowledging faults

In order to acknowledge faults in the message list, proceed as follows:

Procedure

1. In order to acknowledge the faults being displayed, click on the "Acknowledge faults" button.
   The displayed faults are acknowledged. Acknowledged faults continue to be displayed in the message list with the symbol.

A.2.2.3 “Diagnostics buffer” display area

In the “Diagnostics buffer” display area, important operating events are included in the log in the form of a logbook. The relevant data is read out from the non-volatile memory and is available along with its history in the diagnostics buffer for the subsequent analysis of an operating fault.

Displaying the diagnostic buffer

In order to call up the diagnostic buffer, proceed as follows:

Procedure

1. In the navigation, select “Diagnostics > Diagnostics buffer.”
   The logged events are displayed.

Note

In the “Date and time” column, the time - differing from the current drive time - is combined from the following components: "1.1.2000 + Operating hours counter".

Filtering diagnostic buffers

In the event list of the diagnostic buffer, you can set filters, narrowing down the events that are displayed. The filter settings can be configured using the filter list above the event list. All filters are linked by a logical conjunction (AND).

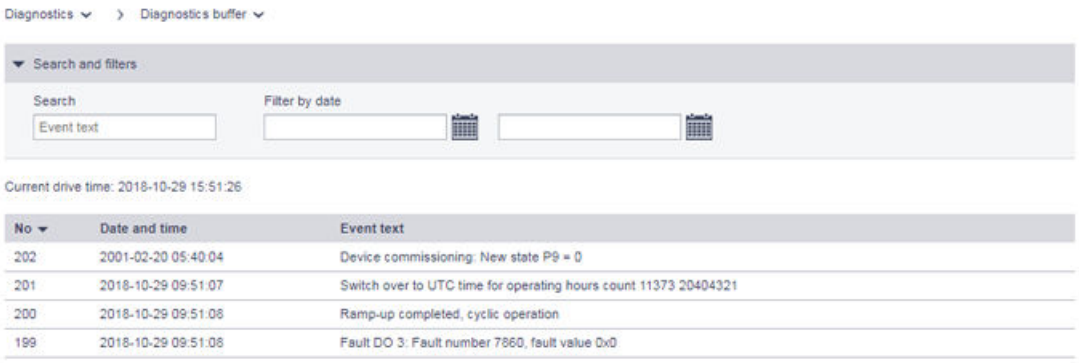


Figure A-75 Example: Filtering diagnostic buffers

Setting filters

Proceed as follows to set the filters in the “Search and filter” filter bar.

Note

Collapsing the filter bar

The filter bar is opened per default. To close the filter bar, click anywhere in the header of the “Search and filter” bar.

Procedure

1. In the "Search" field, enter a search term (any number of characters) for which you want to search in the diagnostic buffer.
   The search results are displayed in the event list.

   Note

   The search term affects the column “Event text” in the event list.

2. In the “Filter by date” fields, specify a date range for which you want to display events.
   After each setting is configured, the search results in the event list are narrowed down further. The filters can be set in any order.

Resetting filters

As long as you are logged in to the web server and the filter settings have not changed, the event list is always displayed with the last filter settings. In order to reset all filter settings in the event list, proceed as follows:

Procedure

1. Click "Reset all filters" at the top right in the filter bar.
   You have now re-set all configured filters. The event list then displays the unfiltered view of the operating events again.

A.2.2.4 "Communication" display area

In order to call up the "Communication" display area, proceed as follows:

Procedure

1. Select "Diagnostics > Communication" in the navigation.
   The web server shows a window with the following contents:
   - IP address of the converter
   - Name of the station
   - Information as to whether the connection between the controller and the converter is active.
   - Table with process data for the transfer direction "controller > converter"
   - Table with process data for the transfer direction "converter > controller"

Figure A-76 Example: Communication display area

The values are displayed in hexadecimal format in the default setting. You can switch the display of individual values between binary and hex format by clicking on the button to the right of the value.

A.2.2.5 "Trace files" display area

The web server permits the loading of trace files that were created using a multiple trace and stored on the memory card of the drive. All the files in the "USER/SINAMICS/DATA/TRACE" directory of the memory card can be loaded to the web client (i.e. to the PC). The loadable trace files are displayed on the web page with their name.

The trace files can be displayed graphically in the engineering tool.

Note

Activation and parameterization of the multiple trace

Detailed information on the activation and parameter assignment of a multiple trace can be obtained in the following documentation:

- SINAMICS S120 Commissioning Manual with Startdrive
- Startdrive information system

Here, you can also obtain detailed information about how you can load trace files into your PC file system.

Loading trace files from the memory card

In order to load trace files from the memory card to your device/computer, proceed as follows:

Procedure

1. In the main menu, click on the "Diagnostics" entry.
2. In the sub-menu, select the "Trace files" option.
   If you have already saved trace files, these are displayed in the list.
3. In the list, select the trace file that you want to load.
   You are then prompted whether you want to open the trace file or store it in your file system.
4. Save the file in your file system.
   The file stored in the file system can be opened with the engineering tool.

A.2.3 Creating and adjusting the parameter list

A.2.3.1 Overview

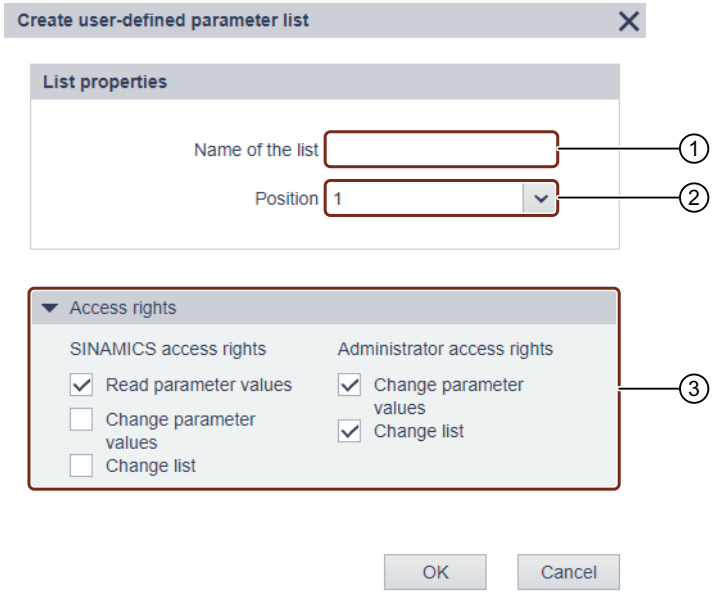
In the web server, you can manage up to 20 parameter lists with 40 parameters each. The created parameter lists are saved on the memory card of the converter and are also available after a restart.

A.2.3.2 Creating a parameter list

Procedure

To create a parameter list, proceed as follows:

1. Click the "Parameter" entry in the navigation.
   The "Parameters" display area opens.
2. Click the "Create list" tab.
   The "Create user-defined parameter list" dialog opens.



① "Name of the list" input field
② "Position" drop-down list
③ "Access rights" setting area (expandable)

3. In the "Name of the list" ① input field, enter a name for the parameter list.
   When assigning license names, only use alphanumeric characters and the special characters specified in brackets (-_+.).
4. In the "Position" drop-down list ② select a position for the parameter list.
   You can create a maximum of 20 parameter lists. If needed, you can change the order of the tabs in the "Parameters" display area (see the "Changing the list properties (Page 309)" chapter).

5. Change the access rights ③ for the "SINAMICS" user if required.
   The "Read parameter values" option is preset in the default settings.
   Observe and adhere to the following instructions if you want to change the access rights of the "SINAMICS" user.
   - Never simultaneously assign a "SINAMICS" user the access rights for the "Change list" and "Change parameter values" functions.
   - Only assign the access rights for the "Change parameter values" function if this is absolutely necessary. The access rights can be extended during creation of a parameter list or via the "List properties" dialog. The extension of the access rights is limited to individual parameter lists and the parameters contained in them. The "Administrator" user can change the access rights for the "SINAMICS" user at any time via the "List properties" dialog (see Chapter "Changing the list properties (Page 309)").
6. In order to save your settings, click "OK".
   The "Create user-define parameter list" is closed and the settings are saved. The created parameter list appears as an empty list at the position that you selected.
   OR
7. To discard your settings, click "Cancel".
   The "Create user-defined parameter list" dialog is closed and the settings are discarded.

A.2.3.3 Adding parameters

Procedure

⚠ WARNING

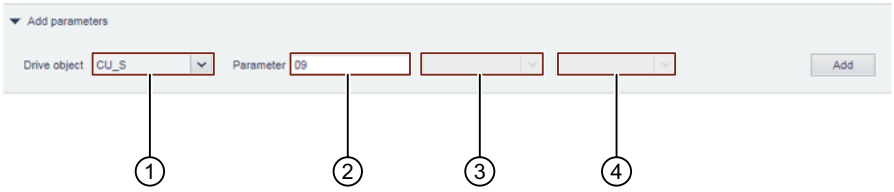
Uncontrolled movement of the drive as a result of incorrect parameter assignment

Incorrect parameterization can cause uncontrolled drive movements, which may result in death or serious injury.

- Make sure that the parameter assignment of the drive objects is correct.

You can add individual parameters to an existing parameter list as follows:

1. Click the "Parameter" entry in the navigation.
   The "Parameters" display area opens.
2. Click anywhere in the "Add parameters" field.
   The entry and selection boxes in the "Add parameters" field are then displayed. The ③ and ④ selection boxes are only activated if index-coded or bit-coded parameters are input.



① Selection box: DO (selection in accordance with the present configuration)
Note: You can only change the name of the drive objects when configuring your drive in the Startdrive engineering tool.
② Input field: Parameter
③ Selection box: Index value (selection of adjustable indices for index-coded parameters)
④ Selection box: Bit value (selection of configurable bits for bit-coded parameters)

3. Enter a parameter into the "Parameter" input field.
   If you enter an invalid parameter, it is highlighted in red. Parameters are indicated as invalid if they do not exist or are not assigned to the selected drive object (e.g. CU_S). Invalid parameters are not added to the parameter list.
   More detailed information on the individual parameters and their assignment to a drive object can be found in the SINAMICS S120/S150 List Manual.
4. If necessary, select the desired bit and/or index for the parameter that was entered.
5. In order to accept the parameter with the selected settings into the parameter list, click "Add" or confirm with "Enter".

The parameter is added to the existing parameter list.

A.2.3.4 Selecting/entering parameters

Procedure

In an existing parameter list, you can select or enter the parameter values for individual parameters in the “Value” column. Proceed as follows:

1. Select the desired value for a parameter from the corresponding drop-down list.
   OR
   Enter the desired value for a parameter into the corresponding entry field.

Additional information

For more information on adjustable parameter values, refer to the SINAMICS S120/S150 list manual.

A.2.3.5 Changing the parameter sequence

In an existing parameter list, you can change the parameter sequence by appropriately dragging & dropping.

A.2.3.6 Deleting parameters

In an existing parameter list, you can delete individual parameters as follows:

1. To delete a parameter, click on the cross symbol ✕ in the corresponding line.
   The “Remove parameter from list” dialog opens.
2. Confirm the deletion operation by clicking “Remove.”
   OR
   Click on “Cancel” to cancel the deletion operation.

A.2.3.7 Changing the list properties

To change the list properties of an existing parameter list, proceed as follows:

1. Click the "Parameter" entry in the navigation.
   The "Parameters" display area opens.
2. Click on the “List properties” button.
   The “List properties" dialog opens.
3. Make your relevant changes.
   You can change the following properties:
   - Name of the list
   - Position of the list in the tab bar.
   - Access rights of the “SINAMICS” user and/or “Administrator”
4. Confirm your changes by clicking "OK".
   The dialog closes.

The changes made are applied.

A.2.3.8 Deleting a parameter list

Proceed as follows to delete a previously existing parameter list:

1. Click the "Parameter" entry in the navigation.
   The "Parameters" display area opens.
2. Select the relevant parameter list in the tab bar.
3. Click on the “List properties” button.
   The “List properties" dialog opens.
4. Click on the “Delete this list” button.
   The “Delete list” dialog opens.
5. Confirm the deletion operation by clicking “Delete this list.”
   The dialog closes.

A.2.4 Backup and restore

Overview

The “Back up and restore” function provides you with the following options:

- Backing up parameters that have been configured.
- Assigning a name to the backup file.
- Restoring parameters from a valid parameter backup and loading them to the drive.
- Resetting the drive to factory settings.

Note

The individual options have their own adjustment areas assigned to them, each with an info box, on the “Back up and restore” screen. Observe and follow all information and instructions in the info boxes.

Procedure

1. To call the function, select "Backup and restore" in the navigation.
   The “Back up and restore” screen is open.

A.2.4.1 Backing up parameters

Overview

You can back up the converter settings externally using the web server.

You can perform the data backup at any time. We recommend a data backup after the commissioning of the converter.

Procedure

Proceed as follows to back up the parameters:

1. Click "Save changes"  in the footer of the web server.
   The settings are saved protected against power failure.
2. Click "Back up parameters" in the "Parameter Backup" setting area.
   The parameters are backed up. A corresponding message is displayed when the data backup is successful.

Note

Defining a storage location for the backup file

Depending on the browser used, a dialog appears in which you can specify where the backup file is to be saved. In some browsers (e.g. Google Chrome), the file is stored in the standard directory for downloads as "Backup.zip" without a prompt for the storage location.

Note

Checking and editing data

The data to be backed up is written to the backup file in a format that cannot be edited; the data cannot be checked or edited.

3. Change the automatically created name of the backup file.
   The backup file can be unambiguously identified based on the assigned name.

A.2.4.2 Restore file parameters

If you load the externally backed-up parameter settings to the converter again, you restore the converter state to the time of the data backup. You can also use the externally backed-up files for a series commissioning.

1. Click "Browse" in the "Restore Parameters From File" setting area.
2. In your file system, select the backup file.
   The backup file is now displayed in the view.
3. Click "Restore" in the "Restore Parameters From File" setting area.
   The data backup is loaded and the converter is restarted. You must log in to the web server again.
4. Log in to the web server again.

A.2.4.3 Restoring the factory setting

Note

You have forgotten the administrator password

If you have forgotten the administrator password, it is not possible to reset the converter to factory settings over the web server. For information on reconfiguring the administrator password, see Chapter "Assigning the administrator password (Page 262)".

Note

Communication settings

If you reset the converter to the factory settings, the IP address of the service interface, the PROFINET IP address and the PROFINET device name are not cleared.

Procedure

In order to reset the converter in the web server to factory settings, proceed as follows:

1. In the "Restore factory settings" setting area, click on "Restore factory settings".
2. Acknowledge the confirmation prompt. The converter is reset, and then restarted.
   If the LED on the converter lights up green, resetting is complete.

You have finished resetting the converter to factory settings. When the web server is called again, the initial setup is started (see Chapter "Assigning the administrator password (Page 262)").

A.2.5 System settings

A.2.5.1 Setting or changing user accounts

Overview

The "SINAMICS" and "Administrator" user roles have been predefined and cannot be changed.

Settings

The following settings are available for the user roles:

User role	Setting	Note
Administrator	Change password	The user cannot be disabled in the web server.
SINAMICS	Enable/lock user	The user is enabled by default.
	Assign password	The user must be enabled.
	Change/delete password	–

Requirements for secure passwords

To protect against unauthorized access, by an attacker, for example, generate a secure password that consists of:

- At least 8 characters
- Uppercase and lowercase letters
- Numbers and special characters (e. g. ?!%+ etc.)
- Different passwords for different user roles

Checking the password

The length of the password is checked by the converter. There is no check for special characters or upper and lower case letters.

Remember the passwords or store the passwords in a safe place that cannot be accessed by unauthorized persons.

Changing the password for the "Administrator" user

You can only disable the "Administrator" user in the Startdrive engineering tool. Further information can be found in the following manual:

- SINAMICS S120 Commissioning Manual with Startdrive

Procedure

To change the password for the "Administrator" user, proceed as follows:

1. Select "System > Settings" in the navigation.
2. Select the "User Accounts" tab.
3. Click "Change password..." for the "Administrator" user.
   A corresponding dialog opens.
4. Enter the passwords as requested in the dialog.
5. Click "Change" to complete the operation.
   If the entered parameters match, the dialog is closed.
6. To save the settings retentively, click  .

Assigning the password for the "SINAMICS" user

Before you assign the password for the "SINAMICS" user, the user must be enabled.

Procedure

To assign the password for the "SINAMICS" user, proceed as follows:

1. Select "System > Settings" in the navigation.
2. Select the "User Accounts" tab.
3. For the "SINAMICS" user, click on "Assign password...".
   A corresponding dialog opens.
4. Enter the password as requested in the dialog.
5. Click "Assign" to complete the operation.
   If the entered parameters match, the dialog is closed.
6. To save the settings retentively, click  .

Changing the password for the "SINAMICS" user

To change the password for the "SINAMICS" user, proceed as follows:

1. Select "System > Settings" in the navigation.
2. Select the "User Accounts" tab.
3. Click "Change password..." for the "SINAMICS" user.
4. Enter the passwords as requested in the dialog.
5. Click "Change" to complete the operation.
   If the entered parameters match, the dialog is closed.
6. To save the settings retentively, click .

Deleting the password for the "SINAMICS" user

Proceed as follows to delete the "SINAMICS" user:

1. Select "System > Settings" in the navigation.
2. Select the "User Accounts" tab.
3. Click "Delete password..." for the "SINAMICS" user.
4. Enter the current password as requested in the dialog.
5. Click "Delete" to complete the operation.
   If the password was entered correctly, the dialog is closed.
6. To save the settings retentively, click .

A.2.5.2 Password forgotten

Overview

Without the password for the "SINAMICS" user or "Administrator", you are locked out of accessing SINAMICS data and functions in the web server.

Requirements

- The password for the "SINAMICS" or "Administrator" user is not known.

Assigning a new password for the "SINAMICS" user.

If you work in the web server as a "SINAMICS" user, and you have misplaced or forgotten your password, then you can request your password from the "Administrator" user. However, this is only possible when the following conditions are satisfied:

- The "Administrator" user is known.
- The "Administrator" user knows the password for the "SINAMICS" user.

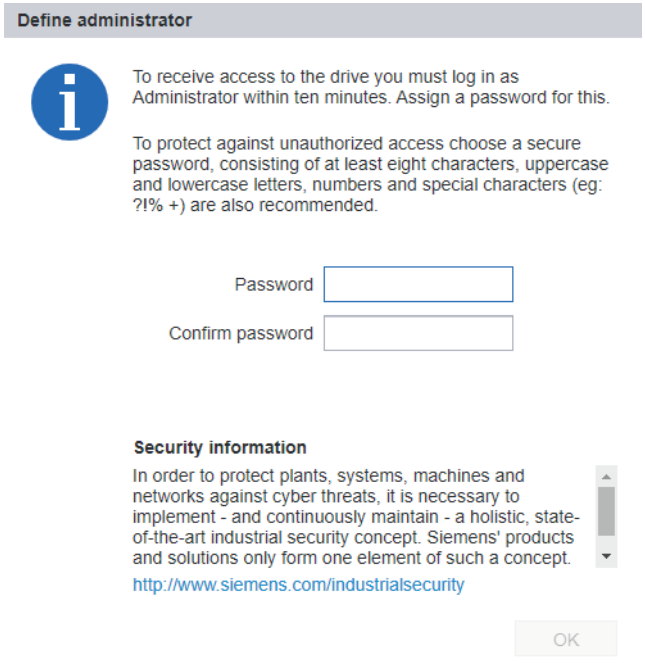
If the "Administrator" user does not know the password for the "SINAMICS" user, then he must generate a new password for the "SINAMICS" user. In this case, the "Administrator" user must

reset the converter to the factory settings in the web server, and then assign a new password for the "Administrator" and "SINAMICS" users.

Procedure

Proceed as follows, to reset the converter in the web server and to assign a new password for the "Administrator" and "SINAMICS" users:

1. Ensure that you as the "Administrator" user are logged into the web server.
   Observe the information displayed in the web server status bar.
2. In the "Restore factory settings" setting area, click on "Restore factory settings".
3. Acknowledge the confirmation prompt. The converter is reset, and then restarted.
   If the LED on the converter lights up green, resetting is complete.
4. Open the browser in your commissioning device.
5. Call the web server using the converter IP address (e.g. 169.254.11.22).
   If you have not assigned a password, then the following dialog is displayed.



6. Enter an administrator password in the "Password" field.

Note

Secure passwords

To protect against unauthorized access, by a hacker, for example, select a secure password that comprises:

- At least 8 characters
- Uppercase and lowercase letters
- Numbers and special characters (e.g.: ?!%+ ...)

It is not permissible that the password is used elsewhere.

Note

Checking passwords

When passwords are entered, the converter only checks the password length. A check is not made for special characters or uppercase/lowercase letters!

7. Repeat the password in the "Confirm password" field.
   If the input is not identical in both fields, the "OK" button is not enabled.
8. Confirm the password that you entered with "OK".
   The display changes to the login page of the web server.
9. Log in using the administrator password.
10. Select "System > Settings" in the navigation.
11. Select the "User Accounts" tab.
12. For the "SINAMICS" user, click on "Assign password...".
    A corresponding dialog opens.
13. Enter the password as requested in the dialog.
14. Click "Assign" to complete the operation.
    If the entered parameters match, the dialog is closed.
15. To save the settings retentively, click on  .
16. Remember the passwords or store them in a secure place that cannot be accessed by unauthorized persons.

Assigning a new password for the "Administrator" user

If you as "Administrator" user have misplaced or forgotten your administrator password, there is no possibility in the web server to assign a new password.

To generate a new administrator password, you must reset the converter in the Startdrive engineering tool and then assign a new administrator password.

As soon as you have generated a new administrator password, and have logged into the web server, when required, you can also generate a new password for the "SINAMICS" user. In this case, proceed as described above.

Procedure

Proceed as follows, to reset the converter in the Startdrive engineering tool and assign a new administrator password:

1. Open the appropriate project in the Startdrive engineering tool.
2. Load the project data from the drive unit to your commissioning device ("Load from device"). By doing this, you secure the current drive configuration in the existing project.
3. Reset the converter to the factory settings.
4. Load the saved drive configuration back into the drive ("Load to device").
5. Open the browser in your commissioning device.
6. Call the web server using the converter IP address (e.g. 169.254.11.22).
   If you have not assigned a password, then the following dialog is displayed.

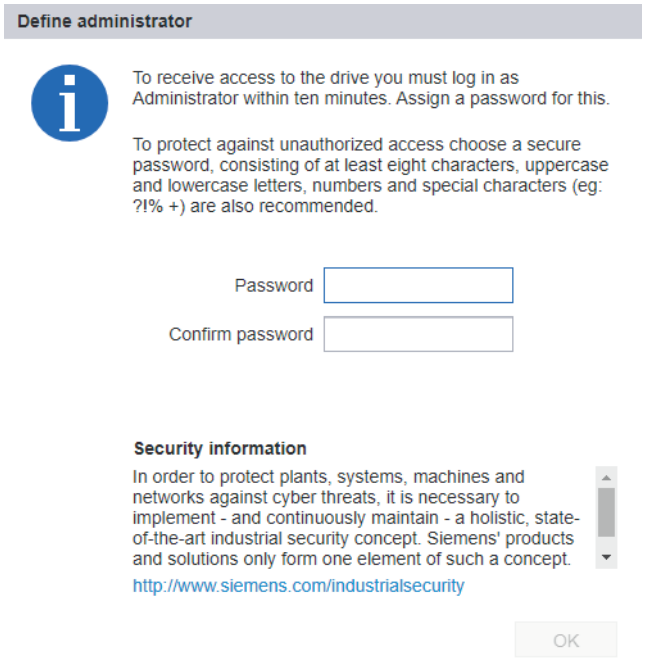


Figure A-77 Prompt to enter the administrator password

7. Enter an administrator password in the "Password" field.

Note

Secure passwords

To protect against unauthorized access, by a hacker, for example, select a secure password that comprises:

- At least 8 characters
- Uppercase and lowercase letters
- Numbers and special characters (e.g.: ?!%+ ...)

It is not permissible that the password is used elsewhere.

Note

Checking passwords

When passwords are entered, the converter only checks the password length. A check is not made for special characters or uppercase/lowercase letters!

8. Repeat the password in the "Confirm password" field.
   If the input is not identical in both fields, the "OK" button is not enabled.
9. Confirm the password that you entered with "OK".
   The display changes to the login page of the web server.
10. Log in using the administrator password.
11. Remember the password or store it in a secure place that cannot be accessed by unauthorized persons.

A.2.5.3 Configuring the IP connection

Overview

Communication between the converter and commissioning device (PG/PC) is established either via an unsecured HTTP connection (see Chapter "Access via service interface X127 (Page 255)") or via a secured HTTPS connection (see Chapter "Access via PROFINET interface X150 (Page 256)").

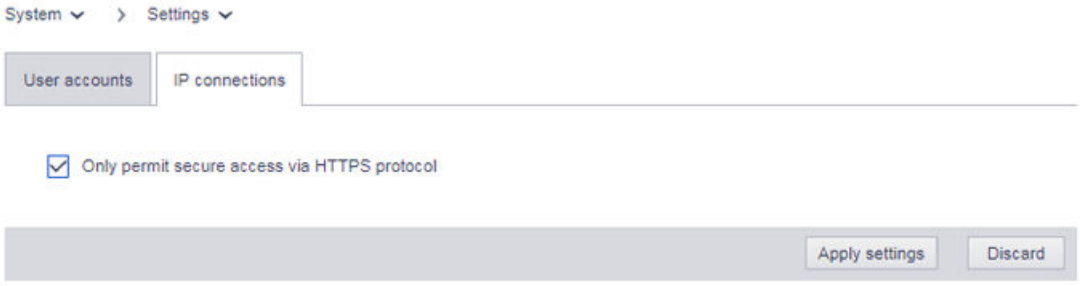
Changing to a secured HTTPS connection

For security reasons, for access via the X127 service interface, we recommend switching over from the unsecured HTTP connection to a secured HTTPS connection.

Proceed as follows:

1. Select "System > Settings" in the navigation.
2. Select the "IP Connections and Addresses" tab.

3. Activate the "Only permit secure access via HTTPS protocol" option.



4. Click "Apply".
   A corresponding dialog opens.
5. Click "OK" to complete the operation.
   If you were logged in via a HTTP connection, you will be logged out of the web server. After this, login is only possible via a secure HTTPS connection.

Note

Certificates for the secure data transfer

To secure an HTTPS connection, it requires security certificates for the encryption of the access. Detailed information on working with these security certificates can be found in Chapter "Using SSL/TLS certificates for secure data transfer (Page 270)".

A.2.5.4 Using functions that require a license

Overview

If you have obtained a license key via the SINAMICS/SINUMERIK Web License Manager, you can enter the license key and activate the license.

Trial License mode

If you have not yet purchased a license key, you can set up and test functions that require a license in Trial License mode.

Requirements

- There is a physical connection (LAN cable) between the commissioning device and the drive.

Display/enter license key

You can view existing license keys on the license overview page of the web server and enter a new license key. Proceed as follows:

1. Select "System > Licenses" in the navigation.
   The license overview page is displayed.
2. In the license overview page, click on "Display/enter license key".
   The corresponding dialog is opened.
   The current license key – if any – is displayed in the upper field of the dialog.
3. Enter the new license key (example: 3SDK-MAGK-AXLC-A) in the "New license key" field.
4. Click on "Activate" to activate the new license key.
   The dialog closes.
   The new license key becomes active on the next ramp-up.

System reactions to under-licensing

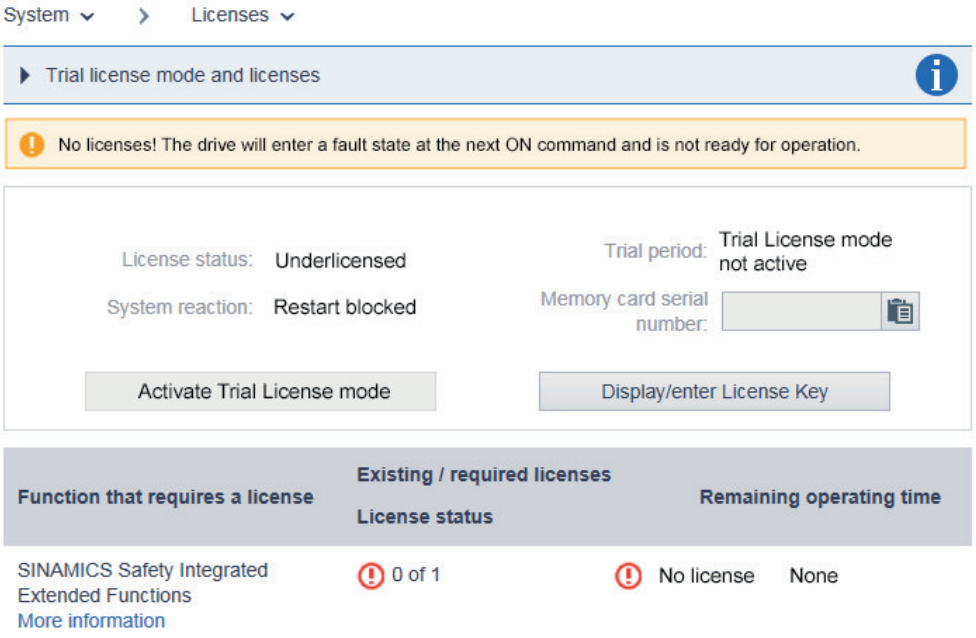
The system responses in case of insufficient licensing are demonstrated using two case examples.

Trial License mode not activated

If licenses are missing for functions that require a license and Trial License mode is not activated, the following system responses are displayed.

- On the converter:
  State is displayed by red flashing (2 Hz) of the RDY LED.

- In the web server:
  - Fault F13000, "Licensing is insufficient"
  - System > Licenses

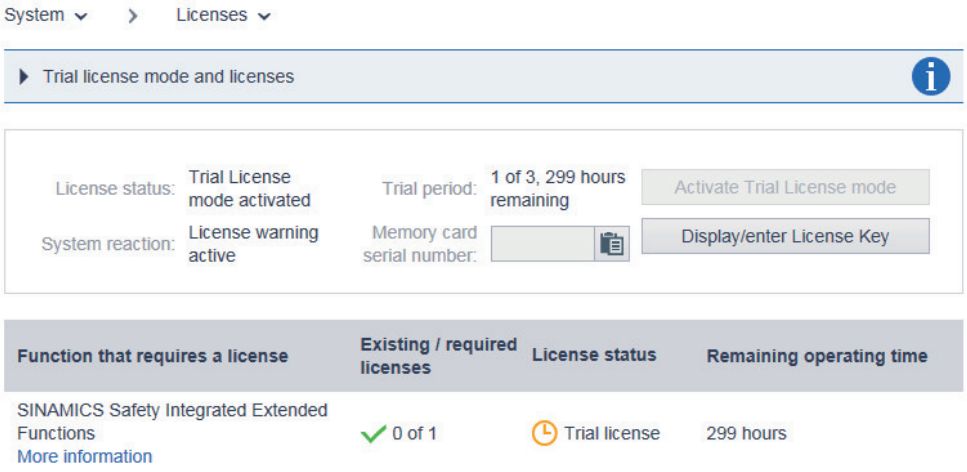


Trial License mode activated

If licenses are missing for functions that require a license and Trial License mode is activated, the following system responses are displayed.

- On the converter:
  State is displayed by red/green flashing (2 Hz) of the RDY LED.

- In the web server:
  - Message A13030 "Trial License activated"
  - System > Licenses



A.2.5.5 Updating the firmware via the web server

Overview

Using the web server, you can upgrade or downgrade the firmware of your drive and load existing STARTER project files onto your drive. The following options are available:

- Loading firmware and STARTER project files into the drive at the same time.
  For information on this, see Chapter "Loading firmware and STARTER project files into the drive (Page 323)".
- Loading firmware and STARTER project files into the drive independently of one another.
  For information on this, see Chapter "Loading STARTER project data into the drive (Page 325)".

Function description

Observe the following information and notes before you upgrade or downgrade the firmware:

Upgrading the firmware

The project-related data is retained when you upgrade the firmware. To retain the web server settings, back up all project-related data in the following directory on the Siemens memory card before the upgrade: **\OEM\SINAMICS\HMI**. Load the saved data back into your drive after the upgrade.

Note

Downgrading a Control Unit

Higher firmware versions are characterized by a larger range of functions. When you downgrade a Control Unit from a higher to a lower firmware version, certain functions may no longer be available.

Downgrading the firmware

When the firmware is downgraded to a lower firmware version, the converter is reset to the factory settings. All project-based data and web server settings are hereby lost.

Protection against power failure

From **firmware version ≥ V4.6**, data on the Siemens memory card is automatically copied from the working partition to a backup partition. This ensures that the data is saved protected against power failure in the event of a fault.

Available firmware versions

You can find the available firmware versions at the following link: SINAMICS S120 firmware (https://support.industry.siemens.com/cs/ww/en/view/109762626).

Loading firmware and STARTER project files into the drive

Requirements

- The firmware is available as ZIP file.
- The STARTER project file is available as ZIP file.
- You can access the ZIP files with your commissioning device (PG/PC, tablet or smartphone).

Procedure

To upgrade the firmware together with existing STARTER project files, do the following:

1. Click on "Firmware update" in the "System" navigation.
   The appropriate dialog opens.

   Note

   Before continuing, observe and follow the instructions and information from the first info box and ensure the following for the duration of the firmware update:
   - The drive(s) are stalled and are not in the "Operation" state.
   - A communication connection is established and the browser is open.
   - The currently open web page cannot be reloaded.

2. Click on "Browse" to the right alongside the "Select firmware/project file" entry field.
3. In the folder directory, select the ZIP file with the firmware version that you wish to load into the drive.
4. If, in addition to the firmware, you also wish to load STARTER project files into the drive, click on "Browse" next to the "Select project file" field.
5. In the folder directory of your commissioning device, select the ZIP file with the STARTER project files that you wish to load into the drive.
6. If you do **not** want to back up the status of the drive before the update, deactivate the "Create system restoration point" option.

   Note

   The "Create system restoration point" option is activated as default setting. If you activate the option, then the present status of the drive is backed up - and in case of fault, can be restored. The status of the drive, backed up in the already existing system restoration point, is then overwritten, and can no longer be restored.

7. Start the firmware update.
   - Checking process:
     During the update, a check is made as to whether there is sufficient free space on the memory card of the drive. The state of the drive objects of the Control Unit is also checked.
   - Alarm and fault messages:
     The alarm "**A01073** POWER ON for backup copy to memory card required" is output if partition 1 and partition 2 on the memory card are not consistent with respect to each other.
     The error message "**F01070** Project/firmware is being downloaded to the memory card" is output for the entire duration of the update.
     You can find entries on alarms and faults in the diagnostics buffer of the CU.

8. The new firmware is installed.
   This process may take several minutes. The CU is restarted after the firmware update has been completed.

RDY	COM	Explanation of the LED displays
		Firmware update is active. • Do not switch off the power supply. • Do not disconnect the motor from the converter.

9. Check whether the new firmware version is installed.
   The firmware version of the drive is displayed on the home page of the web server.

Loading STARTER project data into the drive

Overview

You can load project files created in the STARTER commissioning tool including firmware versions into your drive by means of the "Firmware update" function. The following options are available:

1. Merge the project files incl. firmware versions generated in the STARTER commissioning tool and load them into the drive.
   For information on this, see Chapter "Loading firmware and STARTER project files into the drive (Page 323)".
2. Load the project files generated in the STARTER commissioning tool and load them individually into the drive.
   This option is subsequently described.

Requirement

- The STARTER project file incl. firmware version is available as ZIP file.
- You can access the ZIP file with your commissioning device (PG/PC, tablet or smartphone).

Procedure

Proceed as follows to load a STARTER project file including firmware version into your drive:

1. Click on "Firmware update" in the "System" navigation.
   The appropriate dialog opens.

   Note

   Before continuing, observe and follow the instructions and information from the first info box and ensure the following for the duration of the firmware update:
   - The drive(s) are stalled and are not in the "Operation" state.
   - A communication connection is established and the browser is open.
   - The currently open web page cannot be reloaded.

2. Click on "Browse" to the right of the "Select project file" input field and select the ZIP file with the STARTER project file which you would like to load into the drive.

3. If you do **not** want to back up the status of the drive before the upgrade, deactivate the "Create system restoration point" option.

   Note

   Creating a system restoration point

   The "Create a system restoration point" option is activated as standard. We recommend leaving this option activated at all times.

4. Start the firmware update.
5. The new firmware is installed.
   This process may take several minutes. The Control Unit is restarted after the firmware update has been completed.

RDY	COM	Explanation of the LED displays
		Firmware update is active. • Do not switch off the power supply. • Do not disconnect the motor from the converter.

A.2.5.6 System restoration

Overview

Using the "System restoration" function, you can restore an earlier status of your drive with the help of a generated system restoration point.

Procedure

To restore an earlier status of your drive, proceed as follows:

1. Click on "Firmware update" in the "System" navigation.
   The web server displays the "Firmware update" tab.
2. Click on the "System restoration" tab.
   The "System restoration" screen opens.

   Note

   Before continuing, observe and follow the instructions and information from the first info box and ensure the following for the duration of the firmware update:
   - The drive(s) are stalled and are not in the "Operation" state.
   - A communication connection is established and the browser is open.
   - The currently open web page cannot be reloaded.

3. If you do not want an automatic restart, deactivate the "Execute a restart automatically" option.

Note

Executing a restart automatically

The "Execute a restart automatically" option is activated as standard. We recommend leaving this option activated at all times.

4. To start the system restoration, click on the "Start system restoration" button.

A.3 Write and know-how protection

A.3.1 Write protection

Function description

Write protection prevents unauthorized or inadvertent changes to the settings in the drive.

Activated write protection

Write protection can be activated in offline or online mode. Activated write protection has the following effects:

- Parameters not excluded from write protection cannot be changed.

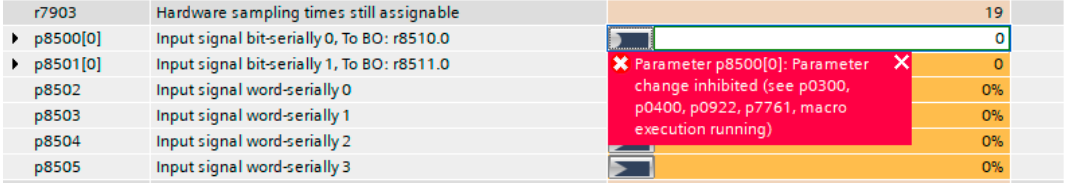


Figure A-78 Message text when write protection is active

- Information regarding the current status of write protection is displayed in the header line of the working area:
  - In online mode, a note is output stating that write protection is activated and therefore no parameters can be written.

Exceptions to write protection

The following parameters are not affected by write protection:

- Parameters with attribute "WRITE_NO_LOCK" are generally not affected by write protection. You can find a list of parameters with the attribute "WRITE_NO_LOCK" in the chapter "Parameters with "WRITE_NO_LOCK"" of the SINAMICS S120/S150 List Manual.

The following functions are not affected by write protection:

- Activate/deactivate write protection
- Change access level (p0003)
- Save parameters (p0971)
- Safely remove memory card (p9400)
- Restore factory settings
- Import settings from an external storage medium (e.g. upload from a memory card)

Parameters (see SINAMICS S120/S150 List Manual)

- r7760.0...12 Write protection/know-how protection status
- p7761 Write protection

A.3.2 Activating/deactivating write protection

Overview

Write protection can be activated in offline or online mode. In online mode, write protection takes effect immediately after activation. We therefore recommend activating write protection in online mode.

Write protection must be deactivated in order to activate or configure know-how protection. However, if necessary, it is possible to activate write protection in addition when know-how protection is activated.

Requirements

- A SINAMICS S120 control module has been inserted in the device configuration.

Procedure

Proceed as follows to activate/deactivate write protection:

1. Establish an online connection to your drive.
2. Call the "Drive control > Parameterization" menu in the project navigator.
3. In the secondary navigation, call "Basic parameterization > Write and know-how protection".
4. Click on "Activate write protection".
   Write protection is activated.
   OR
5. Click on "Deactivate write protection".
   Write protection is deactivated.
6. To save the setting retentively, click  .

A.3.3 Know-how protection

Function description

With the know-how protection function, a machine manufacturer can prevent unauthorized persons from reading, changing or copying confidential company know-how on configuring and parameterizing.

Activated know-how protection

Note

Assistance provided by technical support

When know-how protection is activated, assistance can only be provided by Technical Support after prior agreement from the machine manufacturer.

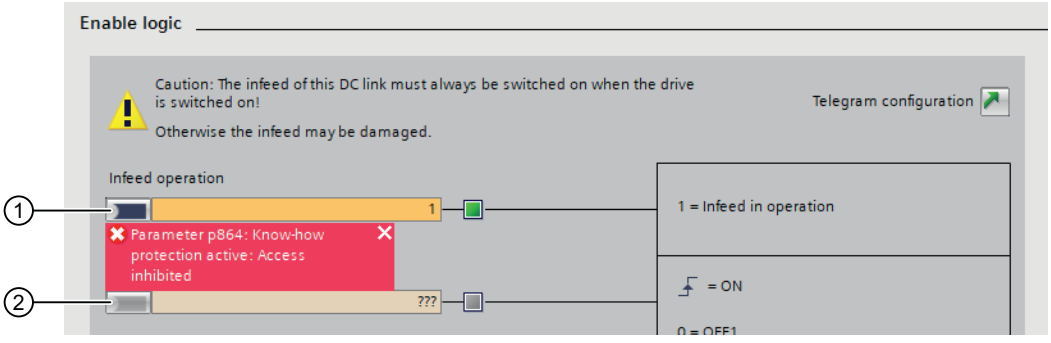
Note

Know-how protection when write protection is active

When write protection is enabled, the protection settings of the know-how protection cannot be changed.

Activated know-how protection has the following effects:

- Parameter view:
  In the parameter view, know-how-protected parameters are not shown in the parameter lists.
- Function view:
  - Know-how-protected parameter values ("KHP_ACTIVE_READ") that can be read but not changed ① are shown but are protected against modification.
  - Know-how protected parameter values that can neither be read nor changed ② are indicated by "???" and are protected against modification.



① Properties: Can be read, cannot be changed (dark orange background)
② Properties: Cannot be changed (light orange background)

- Information regarding the current status of know-how protection is displayed in the header line of the working area:
  - When the "Write and know-how protection" function is called in offline mode, a note is output indicating that know-how protection can only be configured in online mode.
  - In online mode and when know-how protection is activated, a note is output in all screens indicating that know-how protection is active, which means that you cannot read or change all parameters.
- The status of the know-how protection is indicated by the lock icon in the project navigator.

Available protection settings

The following figure shows the protection settings with which drives can be protected against unauthorized access and unauthorized reproduction of the **drive settings (parameter and DCC data)**:

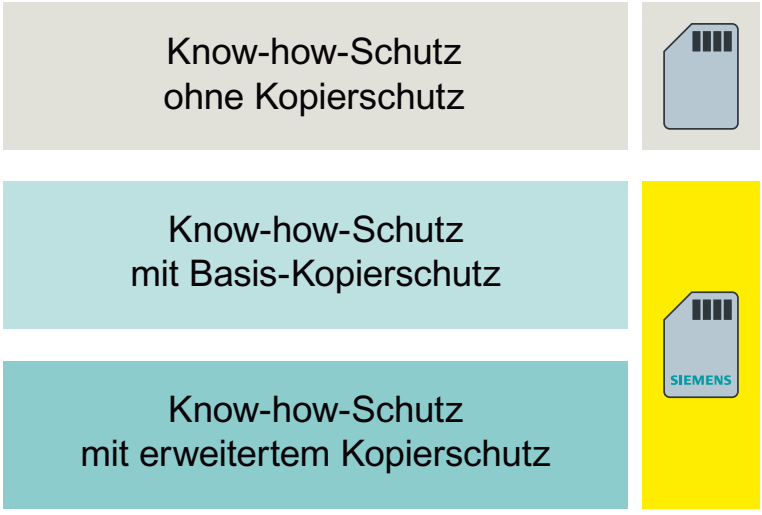


Figure A-79 Available protection settings

Note

Siemens memory card

Use of know-how protection with basic copy protection and extended copy protection is only possible with a Siemens memory card.

Effects during device replacement

The settings serve to protect confidential company know-how on configuration and parameterization and limit the end user's possibilities as follows, according to the selected setting:

- **Know-how protection without copy protection**
  Despite activated know-how protection, the end user can copy the drive settings and transfer them to further Control Units using any memory card.
- **Know-how protection with basic copy protection**
  Know-how protection is bound to the **serial number of the Siemens memory card**. When know-how protection is activated, the know-how-protected drive settings are protected against copying and use on other memory cards.

  Note

  After a device replacement, the converter can be operated with the Siemens memory card from the defective device without knowing the know-how protection password.

- **Know-how protection with extended copy protection**
  Know-how protection is bound to the **serial number of the Siemens memory card and the Control Unit**. When know-how protection is activated, the know-how-protected drive settings are protected against copying and use on other memory cards and Control Units.

  Note

  After a device replacement, the converter can be operated with the Siemens memory card from the defective device only if the know-how protection password is known.

Effects on parameters and functions

The following table provides a detailed overview of the effects of the individual protection settings on parameters and functions with activated know-how protection:

Affected	Protection settings	Description
Adjustable parameters	Readable, changeable	Adjustable parameters without know-how protection (p...) can be read and changed when know-how protection is active. You can find a list of the adjustable parameters that can be read and changed in the SINAMICS S120/S150 List Manual in the chapter "Parameters with "KHP_WRITE_NO_LOCK"". **Note:** Adjustable parameters without know-how protection cannot be added to an exception list (see Chapter "Managing the exception list (Page 336)").
	Readable	Certain adjustable parameters with know-how protection (p...) can be read but not changed when know-how protection is active. You can find a list of the adjustable parameters that can be read in the SINAMICS S120/S150 List Manual in the chapter "Parameters with "KHP_ACTIVE_READ"".

Affected	Protection settings	Description
Functions	Locked	The following functions are locked when know-how protection is activated: • Loading drive settings into the project (function: "Upload from device") • Automatic controller optimization • Stationary or rotating measurement of the motor data identification • Deleting alarm history and fault history • Generating acceptance documents for safety functions
	Executable	The following functions can be executed when know-how protection is activated: • Restoring factory settings • Acknowledging faults • Displaying faults, alarms, fault history and alarm history • Reading out the diagnostic buffer • Controlling the drive via the control panel • Displaying acceptance documents for safety functions
	Optionally executable	The following functions can be executed if the "Allow diagnostic functions" option is enabled when know-how protection is activated: • Trace function • Measurement function

Parameters (see SINAMICS S120/S150 List Manual)

- r7760.0...12 CO/BO: Write protection/know-how protection status
- p7765 KHP password configuration
- p7766[0...29] KHP password input
- p7767[0...29] KHP password new
- p7768[0...29] KHP password confirmation

A.3.4 Configuring know-how protection

Overview

Know-how protection can only be activated and configured in online mode. Therefore, always make sure that there is an online connection to your drive unit before calling the configuration screen for know-how protection.

More information on the individual protection settings can be found in Chapter "Know-how protection (Page 329)".

Requirements

- A SINAMICS S120 control module has been inserted in the device configuration.
- An online connection to the drive has been established.

- Write and know-how protection are disabled.
- A Siemens memory card is inserted in the converter. This requirement applies to know-how protection with basic copy protection and extended copy protection.
- **Optional:**
  - The drive unit is fully commissioned.
  - The exception list for know-how protection is created. No critical parameters have been added to the exception list.

Selecting and activating the protection setting

Proceed as follows to select and activate the desired protection setting:

1. If you have already added know-how parameters to the exception list before activating know-how protection, make sure that you have not added any critical parameters (see Chapter "Managing the exception list (Page 336)").

   Note

   Parameters in the exception list can be read and modified

   With activated know-how protection, parameters in the exception list can be read and modified in other commissioning tools and in the web server. Therefore, do not add any critical parameters to the exception list.

2. Establish an online connection to your drive.
3. Select the "Drive control > Parameters" menu in the project navigator.
4. In the secondary navigation, select menu "Basic parameterization > Write and know-how protection".
   The "Write and know-how protection" screen form is displayed with the available protection settings.
5. Select the required setting.
   The following settings are available:
   - Know-how protection without copy protection (default setting)
   - Basic copy protection
   - Extended copy protection
6. To activate use of diagnostic functions with enabled know-how protection, select the option "Permit trace and measuring functions for diagnostic purposes".

7. To activate know-how protection with the selected protection setting, click "Specify password for the activation".
   The corresponding dialog is opened.
8. Assign a password and confirm with "OK".

Note

Recommendation for secure passwords

When assigning a password, make sure that it contains the following:

- At least 8 characters
- Upper and lower case letters
- Numbers and special characters (e.g. ?!%+)

It is not permissible that the password is used elsewhere.

Know-how protection with the desired protection setting is activated. The know-how protected parameters cannot be changed until know-how protection is deactivated.

Important notes

- Write protection can be activated in addition to activated know-how protection. Make sure that write protection is deactivated before you deactivate know-how protection.
- Know-how protection must be deactivated to be able to change a created exception list.

Changing a password

To change an existing password, proceed as follows:

1. Click the "Change password" button.
   The corresponding dialog is opened.
2. Enter the existing and the new password in the appropriate input fields.
3. Confirm your entries with "OK".

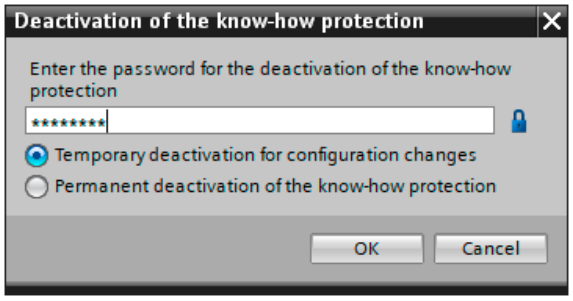
The dialog closes. The new password becomes immediately valid.

Deactivating know-how protection temporarily

Deactivate know-how protection temporarily to change the protection settings and/or the exception list. You can find more information on managing an exception list in Chapter "Managing the exception list (Page 336)".

Proceed as follows to deactivate the know-how protection temporarily:

1. Click on "Deactivation".
   The corresponding dialog is opened. The following options are available:



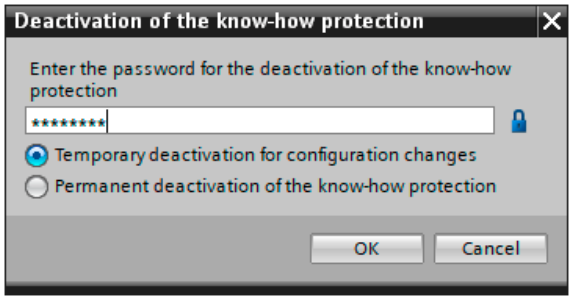
2. Select option "Temporary deactivation for configuration changes" option.
   Know-how protection is deactivated.
3. Enter the existing password for know-how protection.
4. To save the setting retentively, click .

Know-how protection is temporarily deactivated and can be reactivated at any time with the selected protection settings.

Deactivating know-how protection permanently

Proceed as follows to deactivate the know-how protection permanently:

1. Click on "Deactivation".
   The corresponding dialog is opened. The following options are available:



2. Select option "Permanent deactivation of the know-how protection".
   A security prompt is displayed.
3. Enter the existing password for know-how protection.
4. If you want to permanently deactivate know-how protection, confirm the prompt with "Yes".
   Know-how protection is deactivated and the protection settings are reset to the factory settings.
5. To save the setting retentively, click .

Know-how protection is permanently deactivated and can be activated and reconfigured at any time.

Additional protective measures

After configuration of know-how protection, make sure that the Startdrive project file is not retained by the end user.

A.3.5 Managing the exception list

Overview

In the exception list, you manage all parameters that are to remain readable and modifiable with activated know-how protection.

Features

- The exception list can be configured in both online and offline mode.
- The exception list can be called via the parameter lists of the individual drive objects. In the factory setting, the exception list that can be called via the parameter list of the "Drive control" drive object only contains the parameter for the know-how protection password (p7766[0]).

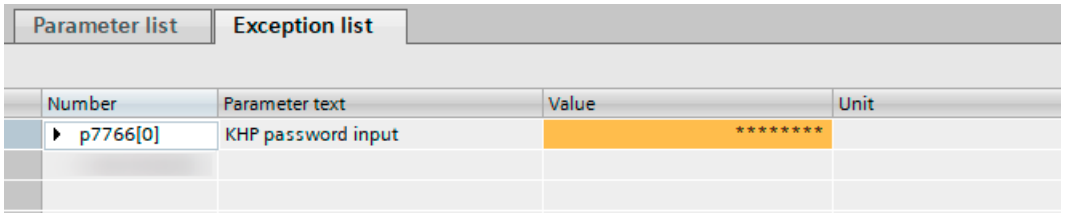


Figure A-80 Exception list with know-how protection password

Note

Deactivation of know-how protection not possible

The parameter for the know-how protection password (p7766[0]) cannot be deleted from the exception list. If this parameter is deleted, know-how protection will remain permanently activated after activation and can no longer be deactivated. In this case, the drive will need to be restored to the factory settings.

Requirements

- Write protection is deactivated.
- Know-how protection is deactivated (either temporarily or permanently).

Adding parameters to the exception list

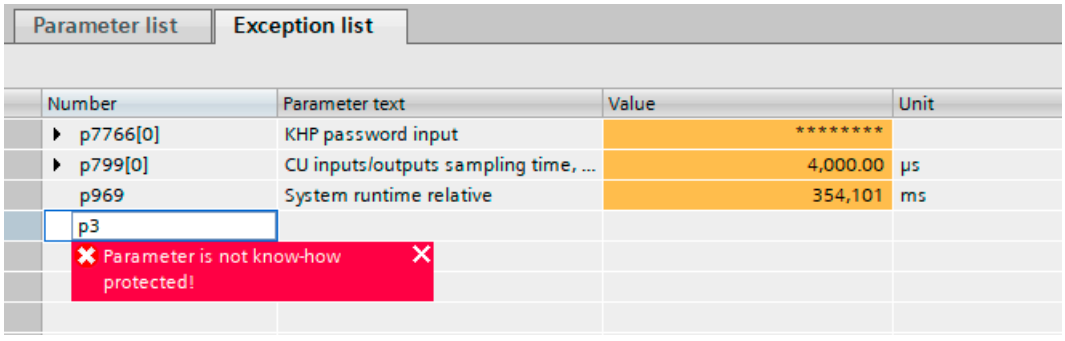
Note

Parameters in the exception list can be read and modified

With activated know-how protection, parameters in the exception list can be read and modified in other commissioning tools and in the web server. Therefore, do not add any critical parameters to the exception list.

Proceed as follows to add individual parameters to the exception list:

1. Establish an online connection to your drive.
2. Call the parameter view of your drive.
3. In the parameter view, click on the icon  .
4. In the "<add new>" input field, enter the parameter number of the know-how protected parameter to be excluded from know-how protection.
   Parameters without know-how protection cannot be added to the exception list.



5. Confirm your entry with Return.
   The most important parameter data is displayed in the exception list.
   The changes in the exception list take effect immediately in online mode.
6. Repeat the process for all other parameters to be excluded from know-how protection.
7. To save the changes in the exception list retentively, click  .
   If you created the exception list in **offline mode**, load the project data into your drive subsequently. The changes in the exception list take effect immediately when you switch to online mode.

After the activation of know-how protection in online mode, only the parameters that were not added to the exception list are know-how protected.

Removing parameters from the exception list

Proceed as follows to remove individual parameters from the exception list:

1. Establish an online connection to your drive.
2. Call the parameter view of your drive.
3. In the parameter view, click on the icon  .
4. In the exception list, select the parameter that you wish to remove from the exception list.

5. Click in the parameter number field, enter "0" and then confirm with Return.
   The complete parameter entry is deleted from the exception list.
   The changes in the exception list take effect immediately in online mode.
6. Repeat the process for all other parameters to be removed from the exception list.
7. To save the changes in the exception list retentively, click  .
   If you remove the parameters from the exception list in **offline mode**, load the project data into your drive subsequently. The changes in the exception list take effect immediately when you switch to online mode.

The modified exception list is taken into account after activation of know-how protection in online mode. All of the parameters that were removed from the list are then know-how protected again.

Parameters (see SINAMICS S120/S150 List Manual)

- p7763 KHP OEM exception list number of indices for p7764
- p7764[0...n] KHP OEM exception list

A.3.6 Overview of important parameters

Note

For a description of the parameters, see the converter List Manual.

Parameter	Function
r7758[0...19]	KHP Control Unit serial number
p7759[0...19]	KHP Control Unit reference serial number
r7760	Write protection / know-how protection status
p7763	KHP OEM exception list number of indices for p7764
p7764[0...n]	KHP OEM exception list
p7765	KHP configuration
p7766[0...29]	KHP password input
p7767[0...29]	KHP password new
p7768[0...29]	KHP password confirmation
p7769[0...20]	KHP memory card reference serial number
r7843[0...20]	Memory card serial number

Service & Support

B

Technical inquiries

Please contact your local partner if you have any technical queries, or wish to request on-site service or spare parts/repairs.

You can find your local partner here (https://www.lda-portal.siemens.com/siemlda/en/contact/form).

Please have the following data ready:

- Type (MLFB)
- Serial number

You can find this data on the rating plate.

References

C

C.1 Additional information

Additional general information about Industrial Security is available here:

- Industrial Security (https://new.siemens.com/global/de/produkte/automatisierung/themenfelder/industrial-security.html)
- Implement Security (https://new.siemens.com/global/en/products/services/industry/digital-industry-services/industrial-security-services.html)
- Operational Guidelines for Industrial Security (https://assets.new.siemens.com/siemens/assets/api/uuid:1c5eebfa-eaef-4d1c-a797-8719bb932559/version:1585555327/dffa-b10556-01-7600-industrial-security-ipdf-en.pdf)

Additional information on assigning secure passwords is provided here:

- National Institute of Standards and Technology (NIST) (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf)
- European Network and Information Security Agency (enisa) (https://www.enisa.europa.eu/media/news-items/basic-security-practices-regarding-passwords-and-online-identities)
- Bundesamt für Sicherheit in der Informationstechnik (BSI) (https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html)[Federal Agency for Security in Information Technology (BSI)] (this is only relevant for Germany)

Additional product-specific information about Industrial Security is available here:

- SINAMICS homepage (https://new.siemens.com/global/en/products/drives/sinamics.html)

Product-specific manuals for the individual products can be found on the Internet:

- LDA Portal (https://www.lda-portal.siemens.com/)

Standards and regulations relating to Industrial Security are available on the Internet.

- IEC 62443

You can find information on the training here:

- Sitrain (https://sitrain.automation.siemens.com/DE/sitrain/default.aspx?AppLang=en), training courses from Siemens for products, systems and solutions in drive and automation technology.

Questions and answers can be found here:

- FAQs (https://support.industry.siemens.com/cs/products?dtp=Faq&mfn=ps&lc=en-DE)
- LDA Portal (https://www.lda-portal.siemens.com/)

Index

A

Access rights
  Web server, 254
Activate write protection
  Online mode, 328
Address
  Setting the PROFIBUS address, 117
Anti-virus program, 35
Application classes, 70
Application security, 20
Assigning a new administrator password
  Web server, 315
Assigning the SINAMICS password
  Web server, 313
Automatic logout
  Web server, 265

B

Benefits, 11

C

Change
  Password, 34
Changing the administrator password
  Web server, 313
Changing the SINAMICS password
  Web server, 314
Changing to a secured HTTPS connection
  Web server, 318
Cloud, 31
Cloud Applications, 31
Cloud computing, 18
Cloud Security, 31
Code analysis, 20
Communication
  Communication services, 44
  Diagnostics, 304
  Dynamic IP address assignment for PROFINET IO, 144
  I&M, 187
  Identification & Maintenance, 187
  Port numbers used, 44
  PROFIdrive, 67
  via Modbus TCP, 188
  via PROFIBUS, 109
Company security, 26
Confidentiality levels, 33
Configuration
  Web server, 253
Configuring the IP connection
  Web server, 318
Control word
  Control word 1, 244
Creating a parameter list
  Web server, 305
Cyclic communication, 244

D

Data
  transporting, 34
Data backup
  Backing up parameters externally, 310
  Restoring the factory setting, 312
  Restoring the parameter data, 311
Data storage, 34
  Encrypting, 34
Data transfer
  PROFINET, 146
  Web server, 253
DCP flashing, 145
Defense in depth, 25
Defense in depth concept, 25
Deleting connectivity module data, 64
Deleting the SINAMICS password
  Web server, 314
Determining the axis number, 93
Determining the object number, 93
Determinism, 140
Device identification, 118
Device name, 143
Diagnostics
  Calling up messages, 300
  Communication, 304
  Displaying device information, 297
  Filter events, 303
  Filtering messages, 301
Diagnostics channel
  Forwarding of messages, 137, 185
Diagnostics channels, 98
Disposal, 65
DMZ network, 28

Documentation
Benefits, 11
Drives
Cyclic data exchange, 107

E

Effects, 19
EIP, 203
Encoder interface
Find reference mark, 77
Flying measurement, 78
EtherNet/IP, 203
Activating X1400 (CBE20), 207
Activating X150 CU320-2 PN, 206
Commissioning the drive, 205
Connect the drive device, 204
Create generic I/O module, 204
Integrating the drive into the EIP network via DHCP (X150), 218
Requirements, 205
Example
PROFIBUS telegram structure, 111
Exchangeable storage media
SINAMICS, 43
Exchangeable storage medium, 34

F

Filter events
Diagnostics, 303
Filtering messages
Diagnostics, 301
Find reference mark, 77
Firewall, 28, 33, 58
Flying measurement, 78
Free telegrams, 73

G

Google Chrome
Secure HTTPS connection, 281
GSD
GSD file, 117

H

Hard disk, 34
Encrypting, 33
Hotfix management, 21
HTTPS connection
SSL/TLS certificate, 270

I

I&M, 187
Identification & Maintenance, 187
IEC 62443, 22
IND (page index), 240, 241
Industrial security
Definition, 17
Objectives, 17
Possible effects, 19
Industrial Security
Threats, 19
Insufficient licensing
System responses, 320
Interface X140
USS, 234
Interfaces
Backing up, 33
Internet Explorer 11
Secure HTTPS connection, 275
Internet of things, 18
Internet of Things, 18
IO controller, 139
IO device, 139
IO supervisor, 139
IoT, 18
IRT, 150, 151
Comparison with RT, 152
ISO 27005, 22

K

Know-how protection
Basic copy protection, 329
Executable functions, 332
Extended copy protection, 329
Locked functions, 332
Online mode, 332
Optionally executable functions, 332
Parameters that can be changed, 331
Readable parameters, 331
SINAMICS, 42
Without copy protection, 329

L

LED
COM, 325, 326
RDY, 325, 326
License key
Display, 320
Enter, 320
Login
Web server, 264
Logout
Web server, 265

M

Manufacturer-specific telegrams, 73
Maximum cable length
USS, 234
MBAP, 195
Media redundancy, 175
Microsoft Edge
Secure HTTPS connection, 281
Mobile device
Measures, 33
Mobile devices, 18
Mobile networks, 18
Mobile terminal device
Locking, 33
Mobile terminal devices
Measures, 33
Modbus Application Header, 195
Modbus TCP, 188
Activate via interface X1400, 191
Activate via interface X150, 191
Communication via data set 47, 198
Function codes used, 195
Mapping tables, 192
Modbus register to the parameters of the Control Unit, 192
Parameterizing communication for X1400, 192
Parameterizing communication for X150, 191
Read and write access, 195
Reading and writing parameters, 197
Motion control with PROFIdrive, 79
Mozilla Firefox
Secure HTTPS connection, 289

N

Network security, 26
Notebook
Measures, 33

O

Online mode
Activate write protection, 328
Know-how protection, 332
Operating hours counter, 248

P

Page index, 241
Parameter channel, 238
IND, 241
Parameter channel"; "IND, 240
Parameter index, 240, 241
Parameter number, 240
Parameters: Access levels
SINAMICS, 42
Password
Change, 34
Characters, 34
Complexity, 34
Inputs, 34
Length, 34
Safe, 34
Password quality, 34
Passwords, 59
Patch management, 21
PC
Measures, 33
Physical production security, 27
Ping snap, 248
Plant security, 26
PLM, 20
PN Gate, 161
Development kit, 164
Requirements, 163
Transferred functions, 162
Ports, 32
Process data, 75
Process data, control words
A_DIGITAL, 70
G1_STW, 70
G2_STW, 70
G3_STW, 70
MT_STW, 71
STW1, 70
STW2, 70

Process data, setpoints
KPC, 70
MOMRED, 71
NSET_A, 70
NSET_B, 70
XERR, 70
Product Lifecycle Management process, 20
Product security notifications, 35
ProductCERT, 21
PROFIBUS, 109
Device identification, 118
Diagnostics, 102
Forwarding of messages via diagnostics channels, 137
Generic station description file, 117
Interface Mode, 76
Master class 1 and 2, 110
Setting the address, 117
Sign-of-life, 125, 160
Slave-to-slave communication, 126
Telegrams, 73
Terminating resistor, 118
VIK-NAMUR, 117
PROFIBUS diagnostics data, 102
Channel-related diagnostics, 105
Data sets DS0/DS1 and diagnostics alarm, 106
Identifier-related diagnostics, 104
Standard diagnostics, 103
Status messages/module status, 104
PROFIBUS telegram structure, 111
PROFIdrive, 67
Controller, Supervisor, Drive Unit, 68
Device classes, 68
Message classes, 98
Message classes for PROFINET, 99
PROFIBUS message classes, 102
Reading parameters, 94
Telegrams, 73
Write parameter, 96
PROFIenergy, 178
Access point, 179
Certification, 178
Commands, 182
PROFINET
Connection channels, 147
Data transfer, 146
Diagnostics, 99
Forwarding of messages via diagnostics channels, 185
Structure example of a system redundancy, 177
System redundancy, 175
With two controllers, 165
PROFINET IO, 139
Addresses, 141
IRT, 150
With IRT, 141
With RT, 140
PROFINET Gate, 161
Protection levels, 26
Protection zone, 28
Protective measures, 60
Pulse cancellation, 244
Pulse enable, 244

R

Real-time communication, 140
Realtime protection, 58
Regulations, 22
Remote access, 18
Ring topology, 175
Scalance, 175
Risk analysis, 23
RT
Comparison with IRT, 152
RT classes
Send cycles, 153
Setting, 152
Update cycles, 153

S

Saving changes protected against power failure
Web server, 269
SCALANCE S, 29
Secure HTTPS connection
Google Chrome, 281
Internet Explorer 11, 275
Microsoft Edge, 281
Mozilla Firefox, 289
Security audit, 23
Security by Design, 20
Security holes, 19
Security integrity, 21
Security module
SCALANCE S, 29
Security service, 20
Security support, 20
Sequence of objects in the telegram, 110, 146
Services, 32
Setting
SINAMICS time synchronization, 251
Setting recovery points, 62

Shared device, 165
SI HSC, 22
SIEM system, 21
Siemens Industrial Holistic Security Concept, 21
    Business Impact Assessment, 22
    Monitoring of residual risk, 22
    Scope, 22
    Target Protection Level, 22
SINAMICS
    Exchangeable storage media, 43
    Know-how protection, 42
    Parameters: Access levels, 42
    Software manipulation, 43
    Virus protection, 43
    X140, 48
SINAMICS Link
    Activation, 227
    Bus cycle, 223
    Configuration example, 230
    Configuring, 223
    Requirements, 221
    Synchronous cycle, 223
    Transmission time, 222
SINAMICS time synchronization
    Setting, 251
Slave-to-slave communication
    Faults, 137
    PROFIBUS, 126
    Setting in HW Config, 131
Software manipulation
    SINAMICS, 43
SSL/TLS certificate
    HTTPS connection, 270
Standard telegrams, 73
Standards, 22
Status word
    Status word 1, 245
STW1 (control word 1), 244
Subindex, 240, 241
Supported Internet browsers
    Web server, 254
Switches for PROFIBUS address, 117
Switching on inhibited, 245
Synchronization domain, 152
Synchronization, ping snap, 248
System integrity, 26
System redundancy, 175
    Configuring, 177
    Diagnostics LEDs, 177
    Example, 177
System responses
    Insufficient licensing, 320

T

Tablet PCs, 18
Telegram configuration, 107
Telegrams
    Manufacturer-specific, 73
    Sequence of objects, 110, 146
    Standard, 73
    Structure, 75
Threat and Risk Analysis, 20
Threats, 19
Time stamp, 248
Time synchronization, 248
TRA, 20
Transport
    Data, 34
Trojans, 35
Type of connection, 178

U

USB port lock, 33
USB stick, 34
User accounts, 32
USS
    Interface X140, 234
    Maximum cable length, 234
USS (universal serial interface), 233, 238

V

Virus protection
    SINAMICS, 43
Virus protection program, 35
Virus scanner, 35
Viruses, 35

W

Web server
    Access rights, 254, 258
    Assigning a new administrator password, 315
    Assigning the SINAMICS password, 313
    Automatic logout, 265
    Changing the administrator password, 313
    Changing the SINAMICS password, 314
    Changing to a secured HTTPS connection, 318
    Configuration, 253
    Configuring the IP connection, 318

Configuring user accounts, 312
Creating a parameter list, 305
Data backup, 310
Data transfer, 253
Deleting the SINAMICS password, 314
Initial login, 262
Login, 264
Logout, 265
Restoring the data backup, 311
Restoring the factory setting, 312
Saving changes protected against power failure, 269
Support information, 268
Supported Internet browsers, 254
User roles, 258
Windows backup, 58
Windows Security Center, 58
Windows Server Update Service, 36
Windows update, 58
Windows updates, 58
Wireless technology, 18
Worms, 35
WSUS, 36

X

X140
SINAMICS, 48

Z

ZSW1 (status word 1), 245

Further Information

www.siemens.com/LDA

Siemens AG
Large Drives Applications
Vogelweiherstr. 1-15
90441 NÜRNBERG
Germany