WAGO TECHDOCS

Manual

WAGO I/O System 750



750-8100

PFC100; 2ETH; ECO

Controller PFC100; 2 x ETHERNET; ECO

Version 1.12.0, valid from FW Version 03.10.08(22)

© 2022 WAGO GmbH & Co. KG
All rights reserved.

WAGO GmbH & Co. KG

Hansastraße 27
D-32423 Minden

Phone: +49 (0) 571/8 87 – 0
Fax: +49 (0) 571/8 87 – 1 69

E-Mail: info@wago.com

Web: www.wago.com

Technical Support

Phone: +49 (0) 571/8 87 – 4 45 55
Fax: +49 (0) 571/8 87 – 84 45 55

E-Mail: support@wago.com

Every conceivable measure has been taken to ensure the accuracy and completeness of this documentation. However, as errors can never be fully excluded, we always appreciate any information or suggestions for improving the documentation.

E-Mail: documentation@wago.com

We wish to point out that the software and hardware terms as well as the trademarks of companies used and/or mentioned in the present manual are generally protected by trademark or patent.

WAGO is a registered trademark of WAGO Verwaltungsgesellschaft mbH.

Table of Contents

1 Notes about this Documentation 11
1.1 Validity of this Documentation 11
1.2 Copyright 11
1.3 Property rights 12
1.4 Symbols 14
1.5 Number Notation 16
1.6 Font Conventions 16
2 Important Notes 17
2.1 Legal Bases 17
2.1.1 Subject to Changes 17
2.1.2 Personnel Qualifications 17
2.1.3 Use of the 750 Series in Compliance with Underlying Provisions 17
2.1.4 Technical Condition of Specified Devices 18
2.2 Safety Advice (Precautions) 19
2.3 Licensing Terms of the Software Package Used 22
2.4 Special Use Conditions for ETHERNET Devices 22
3 Overview 24
4 Properties 27
4.1 Hardware Description 27
4.1.1 View 27
4.1.2 Labeling 29
4.1.2.1 Production Code 29
4.1.3 Connectors 30
4.1.3.1 Service Interface 30
4.1.3.2 Network Connectors 31
4.1.3.3 Wiring Level 32
4.1.4 System Contacts 33
4.1.4.1 Data Contacts 33
4.1.5 Display Elements 34
4.1.5.1 System/Fieldbus LEDs 34
4.1.5.2 Network Connector LEDs 35
4.1.5.3 Memory Card Slot LED 36
4.1.6 Operating Elements 37
4.1.6.1 Address Selection Switch 37
4.1.6.2 Operating Mode Switch 38
4.1.6.3 Reset Button 39
4.2 Slot for Memory Card 40
4.3 Schematic Diagram 41
4.4 Technical Data 42
4.4.1 Mechanical Data 42
4.4.2 System Data 42
4.4.3 Power Supply 42
4.4.4 Clock 43
4.4.5 Programming 43
4.4.6 Local Bus 43

4.4.7 ETHERNET 43
4.4.8 Connection Type 44
4.4.9 Climatic Environmental Conditions 44
4.5 Approvals 45
4.6 Standards and Guidelines 47

5 Function Description 48

5.1 Network 48
5.1.1 Interface Configuration 48
5.1.1.1 Operation in Switch Mode 48
5.1.1.2 Operation with Separate Network Interfaces 48
5.1.2 Network Security 50
5.1.2.1 Users and Passwords 50
5.1.2.1.1 Services and Users 50
5.1.2.1.2 WBM User Group 51
5.1.2.1.3 Linux User Group 52
5.1.2.1.4 SNMP User Group 52
5.1.2.2 Web Protocols for WBM Access 53
5.1.2.2.1 TLS Encryption 53
5.1.2.3 Root Certificates 55
5.1.3 Network Configuration 56
5.1.3.1 Host Name/Domain Name 56
5.1.3.2 Routing 56
5.1.4 Network Services 60
5.1.4.1 DHCP-Client 60
5.1.4.2 DHCP Server 60
5.1.4.3 DNS Server 62
5.1.5 Cloud Connectivity Functionality 63
5.1.5.1 Components of the Cloud Connectivity Software Package 64
5.2 Memory Card Function 65
5.2.1 Formatting 65
5.2.2 Data Backup 66
5.2.2.1 Backup Function 66
5.2.2.2 Restore Function 67
5.2.3 Inserting a Memory Card during Operation 69
5.2.4 Removing the Memory Card during Operation 69
5.2.5 Setting the Home Directory for the Runtime System 70
5.2.6 Load Boot Project 70

6 Mounting 72

6.1 Installation Position 72
6.2 Overall Configuration 72
6.3 Mounting onto Carrier Rail 74
6.3.1 Carrier Rail Properties 74
6.3.2 WAGO DIN Rails 75
6.4 Spacing 75
6.5 Mounting Sequence 76
6.6 Inserting Devices 77
6.6.1 Inserting the Controller 77

7 Connect Devices 78

7.1 Connecting a Conductor to the CAGE CLAMP® 78
7.2 Power Supply Concept 79
7.2.1 Overcurrent Protection 79
7.2.2 Supplementary Power Supply Regulations 80

8 Commissioning 81

8.1 Switching On the Controller 81
8.2 Determining the IP Address of the Host PC 83
8.3 Setting an IP Address 84
8.3.1 Assigning an IP Address using DHCP 85
8.3.2 Changing an IP Address Using the “CBM” Configuration Tool and a Terminal Program 86
8.3.3 Changing an IP Address using “WAGO Ethernet Settings” 89
8.3.4 Setting the IP Address with the Address Selection Switch 91
8.3.5 Temporarily Setting Fixed IP Addresses 93
8.4 Testing the Network Connection 94
8.5 Changing Passwords 95
8.6 Shutdown/Restart 96
8.7 Initiating Reset Functions 97
8.7.1 Warm Start Reset 97
8.7.2 Cold Start Reset 97
8.7.3 Software Reset 97
8.7.4 Controller Reset 97
8.8 Configuration 99
8.8.1 Configuration via Web-Based-Management (WBM) 100
8.8.1.1 WBM User Administration 102
8.8.1.2 General Information about the Page 105
8.8.2 Configuration via Console-Based-Management-Tool (CBM) using a Terminal Program 107
8.8.2.1 CBM Menu Structure Overview 108
8.8.3 Configuration using “WAGO Ethernet Settings” 111
8.8.3.1 Identification Tab 113
8.8.3.2 Network Tab 114
8.8.3.3 PLC Tab 116
8.8.3.4 Status Tab 117

9 *e!RUNTIME* Runtime Environment 118

9.1 General Notes 118
9.2 CODESYS V3 Priorities 119
9.3 Memory Spaces under *e!RUNTIME* 120
9.3.1 Program and Data Memory 120
9.3.2 Function Block Limitation 120
9.3.3 Remanent Memory 120

10 Modbus – *e!RUNTIME* 121

10.1 Modbus Address Overview 121
10.2 Modbus Registers 122
10.2.1 Modbus Watchdog 124
10.2.1.1 Register 0xFA00 – Watchdog Command 126
10.2.1.2 Register 0xFA01 – Watchdog Timeout 127
10.2.1.3 Register 0xFA02 – Watchdog Status 127

10.2.1.4 Register 0xFA03 – Watchdog Config 128
10.2.1.5 Modbus TCP Connection Watchdog Register 129
10.2.2 Status Registers 130
10.2.2.1 PLC Status Register 130
10.2.3 Electronic Nameplate 130
10.2.3.1 Order Number 130
10.2.3.2 Firmware Version 130
10.2.3.3 Hardware Version 130
10.2.3.4 Firmware Loader/Boot Loader 130
10.2.4 Modbus Process Image Version 130
10.2.5 Modbus Process Image Registers 130
10.2.6 Constant Registers 131
10.2.7 Live Register 131
10.3 Estimating the Modbus Master CPU Load 132

11 Diagnostics 133

11.1 Operating and Status Messages 133
11.1.1 System/Fieldbus LEDs 133
11.1.1.1 SYS LED 133
11.1.1.2 RUN LED 134
11.1.1.3 I/O LED 136
11.1.1.4 MS LED 137
11.1.2 Network Connection LEDs 138
11.1.2.1 LNK LED 138
11.1.2.2 ACT LED 138
11.1.3 Memory Card Slot LED 139
11.2 Diagnostics Messages via Flashing Sequences 140
11.2.1 Flashing Sequences 140
11.2.2 Example of a Diagnostics Message Indicated by a Flashing Sequence 141
11.2.3 Meaning of Blink Codes and Procedures for Troubleshooting 142
11.2.4 Meaning of Blink Codes and Procedures for Troubleshooting 148

12 Service 149

12.1 Inserting and Removing the Memory Card 149
12.1.1 Inserting the Memory Card 149
12.1.2 Removing the Memory Card 149
12.2 Firmware Changes 151
12.2.1 Use *e!COCKPIT* to Update/Downgrade the Firmware 152
12.2.2 Use WAGOupload to Update/Downgrade the Firmware 153
12.2.3 Perform Firmware Update/Downgrade 154
12.3 Updating Root Certificates 155

13 Removal 156

13.1 Removing Devices 156
13.1.1 Removing the Controller 156

14 Disposal 157

14.1 Electrical and electronic equipment 157
14.2 Packaging 157

15 Use in Hazardous Environments 159

15.1 Marking Configuration Examples 160
15.1.1 Marking for Europe According to ATEX and IECEx 160
15.1.2 Marking for the United States of America (NEC) and Canada (CEC) 164
15.2 Installation Regulations 167
15.2.1 Special Notes including Explosion Protection 167
15.2.2 Special Notes Regarding ANSI/ISA Ex 169

16 Appendix 170

16.1 Configuration Dialogs 170
16.1.1 Web-Based-Management (WBM) 170
16.1.1.1 “Information” Tab 170
16.1.1.1.1 “Device Status” Page 170
16.1.1.1.2 “Vendor Information” Page 172
16.1.1.1.3 “PLC Runtime Information” Page 173
16.1.1.1.4 “WAGO Software License Agreement” Page 175
16.1.1.1.5 “Open Source Licenses” Page 176
16.1.1.1.6 “WBM Third Party License Information” Page 177
16.1.1.1.7 “Trademarks Information” Page 178
16.1.1.1.8 “WBM Version” Page 179
16.1.1.2 “Configuration” Tab 180
16.1.1.2.1 “PLC Runtime Configuration” Page 180
16.1.1.2.2 “TCP/IP Configuration” Page 183
16.1.1.2.3 “Ethernet Configuration” Page 185
16.1.1.2.4 Configuration of Host and Domain Name” Page 188
16.1.1.2.5 “Routing” Page 190
16.1.1.2.6 “Clock Settings” Page 195
16.1.1.2.7 “Configuration of Service Interface” Page 197
16.1.1.2.8 “Create Bootable Image” Page 198
16.1.1.2.9 “Firmware Backup” Page 199
16.1.1.2.10 “Firmware Restore” Page 201
16.1.1.2.11 “Active System” Page 203
16.1.1.2.12 “Mass Storage” Page 204
16.1.1.2.13 “Software Uploads” Page 205
16.1.1.2.14 “Configuration of Network Services” Page 206
16.1.1.2.15 “Configuration of NTP Client” Page 208
16.1.1.2.16 “PLC Runtime Services” Page 209
16.1.1.2.17 “SSH Server Settings” Page 211
16.1.1.2.18 “DHCP Server Configuration” Page 212
16.1.1.2.19 “Configuration of DNS Server” Page 213
16.1.1.2.20 “Status overview” Page 214
16.1.1.2.21 “Configuration of Connection <n>” Page 215
16.1.1.2.22 “Configuration of General SNMP Parameters” Page 221
16.1.1.2.23 “Configuration of SNMP v1/v2c Parameters” Page 222
16.1.1.2.24 “Configuration of SNMP v3 Users” Page 224
16.1.1.2.25 “WBM User Configuration” Page 226
16.1.1.3 “Fieldbus” Tab 227
16.1.1.3.1 “OPC UA Status” Page 227
16.1.1.3.2 “OPC UA Configuration” Page 228
16.1.1.3.3 “OPC UA Server Certificates” Page 231
16.1.1.3.4 “MODBUS Services Configuration” Page 233

16.1.1.4 “Security” Tab ... 234
16.1.1.4.1 “OpenVPN / IPsec Configuration” Page ... 234
16.1.1.4.2 “General Firewall Configuration” Page ... 236
16.1.1.4.3 “Interface Configuration” Page ... 237
16.1.1.4.4 “Configuration of MAC Address Filter” Page ... 238
16.1.1.4.5 “Configuration of User Filter” Page ... 240
16.1.1.4.6 “Certificates” Page ... 242
16.1.1.4.7 “Security Settings” Page ... 243
16.1.1.4.8 “Advanced Intrusion Detection Environment (AIDE)” Page ... 244
16.1.1.5 “Diagnostic” Tab ... 246
16.1.1.5.1 “Diagnostic Information” Page ... 246
16.1.2 Console-Based-Management (CBM) ... 247
16.1.2.1 “Information” Menu ... 247
16.1.2.1.1 “Information” > “Controller Details” Submenu ... 247
16.1.2.1.2 “Information” > “Network Details” Submenu ... 248
16.1.2.2 “PLC Runtime” Menu ... 249
16.1.2.2.1 “PLC Runtime” > “Information” Submenu ... 249
16.1.2.2.2 “Information” > “Runtime Version” Submenu ... 249
16.1.2.2.3 “PLC Runtime” > “General Configuration” Submenu ... 250
16.1.2.2.4 “General Configuration” > “PLC Runtime Version” Submenu 250
16.1.2.2.5 “General Configuration” > “Home Dir On SD Card” Submenu 251
16.1.2.2.6 “PLC Runtime” > “WebVisu” Submenu ... 252
16.1.2.3 “Networking” Menu ... 253
16.1.2.3.1 “Networking” > “Host/Domain Name” Submenu ... 253
16.1.2.3.2 “Host/Domain Name” > “Hostname” Submenu ... 254
16.1.2.3.3 “Host/Domain Name” > “Domain Name” Submenu ... 254
16.1.2.3.4 “Networking” > “TCP/IP” Submenu ... 254
16.1.2.3.5 “TCP/IP” > “IP Address” Submenu ... 255
16.1.2.3.6 “IP Address” > “Xn“ Submenu ... 255
16.1.2.3.7 “TCP/IP” > “Default Gateway” Submenu ... 256
16.1.2.3.8 “Default Gateway” > “Default Gateway n” Submenu ... 256
16.1.2.3.9 “TCP/IP” > “DNS Server” Submenu ... 257
16.1.2.3.10 “Networking” > “Ethernet” Submenu ... 257
16.1.2.3.11 “Ethernet” > “Switch Configuration” Submenu ... 258
16.1.2.3.12 “Ethernet” > “Ethernet Ports” Submenu ... 258
16.1.2.3.13 “Ethernet Ports” > “Interface Xn” Submenu ... 259
16.1.2.4 “Firewall” Menu ... 260
16.1.2.4.1 “Firewall” > “General Configuration” Submenu ... 261
16.1.2.4.2 “General Configuration” > “Interface xxx” Submenu ... 262
16.1.2.4.3 “Firewall” > “MAC Address Filter” Submenu ... 264
16.1.2.4.4 “MAC Address Filter” > “MAC address filter whitelist” Submenu 265
16.1.2.4.5 “MAC address filter whitelist” > “Add new / No (n)” Submenu 265
16.1.2.4.6 “Firewall” > “User Filter” Submenu ... 266
16.1.2.4.7 “User Filter” > “Add New / No (n)” Submenu ... 267
16.1.2.5 “Clock” Menu ... 268
16.1.2.6 “Administration” Menu ... 269
16.1.2.6.1 “Administration” > “Users” Submenu ... 270
16.1.2.6.2 “Administration” > “Create Image” Submenu ... 270
16.1.2.7 “Package Server” Menu ... 271
16.1.2.7.1 “Package Server” > “Firmware Backup” Submenu ... 271

16.1.2.7.2 “Firmware Backup” > “Auto Update Feature” Submenu 272
16.1.2.7.3 “Firmware Backup” > “Destination” Submenu..... 272
16.1.2.7.4 “Package Server” > “Firmware Restore” Submenu 273
16.1.2.7.5 “Firmware Restore” > “Select Package” Submenu 273
16.1.2.7.6 “Package Server” > “System Partition” Submenu..... 274
16.1.2.8 “Mass Storage” Menu 275
16.1.2.8.1 “Mass Storage” > “SD Card” Submenu 275
16.1.2.9 “Software Uploads” Menu 276
16.1.2.10 “Ports and Services” Menu 277
16.1.2.10.1 “Ports and Services” > “Telnet” Submenu 278
16.1.2.10.2 “Ports and Services” > “FTP” Submenu 278
16.1.2.10.3 “Ports and Services” > “FTPS” Submenu..... 279
16.1.2.10.4 “Ports and Services” > “HTTP” Submenu..... 279
16.1.2.10.5 “Ports and Services” > “HTTPS” Submenu 280
16.1.2.10.6 “Ports and Services” > “NTP” Submenu..... 280
16.1.2.10.7 “Ports and Services” > “SSH” Submenu..... 281
16.1.2.10.8 “Ports and Services” > “TFTP” Submenu 281
16.1.2.10.9 “Ports and Services” > “DHCPD” Submenu 282
16.1.2.10.10 “DHCPD” > “Xn” Submenu..... 282
16.1.2.10.11 “Ports and Services” > “DNS” Submenu..... 283
16.1.2.10.12 “Ports and Services” > “IOCHECK PORT” Submenu 284
16.1.2.10.13 “Ports and Services” > “Modbus TCP” Submenu 284
16.1.2.10.14 “Ports and Services” > “Modbus UDP” Submenu 285
16.1.2.10.15 “Ports and Services” > “OPC UA” Submenu 285
16.1.2.10.16 “…” > “Firewall Status” Submenu..... 286
16.1.2.10.17 “Ports and Services” > “PLC Runtime Services” Submenu.... 287
16.1.2.10.18 “PLC Runtime Services” > “e!RUNTIME” Submenu 287
16.1.2.11 “SNMP” Menu..... 288
16.1.2.11.1 “SNMP” > “General SNMP Configuration” Submenu..... 288
16.1.2.11.2 “SNMP” > “SNMP v1/v2c Manager Configuration” Submenu 289
16.1.2.11.3 “SNMP” > “SNMP v1/v2c Trap Receiver Configuration” Submenu 289
16.1.2.11.4 “SNMP” > “SNMP v3 Configuration” Submenu..... 290
16.1.2.11.5 “SNMP” > “(Secure)SNMP firewalling” Submenu 291
16.2 Process Data Architecture 292
16.2.1 Digital Input Modules..... 293
16.2.1.1 1 Channel Digital Input Module with Diagnostics 293
16.2.1.2 2 Channel Digital Input Modules 293
16.2.1.3 2 Channel Digital Input Module with Diagnostics 293
16.2.1.4 2 Channel Digital Input Module with Diagnostics and Output Process Data..... 294
16.2.1.5 4 Channel Digital Input Modules 294
16.2.1.6 8 Channel Digital Input Modules 294
16.2.1.7 8 Channel Digital Input Module NAMUR with Diagnostics and Output Process Data 295
16.2.1.8 8 Channel Digital Input Module PTC with Diagnostics and Output Process Data..... 296
16.2.2 16 Channel Digital Input Modules 297
16.2.2.1 Digital Output Modules 298
16.2.2.2 1 Channel Digital Output Module with Input Process Data..... 298

16.2.2.3 2 Channel Digital Output Modules 298
16.2.2.4 2 Channel Digital Input Modules with Diagnostics and Input Process Data 299
16.2.2.5 4 Channel Digital Output Modules 300
16.2.2.6 4 Channel Digital Output Modules with Diagnostics and Input Process Data 300
16.2.2.7 8 Channel Digital Output Module 300
16.2.2.8 8 Channel Digital Output Modules with Diagnostics and Input Process Data 301
16.2.2.9 16 Channel Digital Output Modules 301
16.2.2.10 8 Channel Digital Input/Output Modules 302
16.2.3 Analog Input Modules 303
16.2.3.1 1 Channel Analog Input Modules 303
16.2.3.2 2 Channel Analog Input Modules 303
16.2.3.3 2 Channel Analog Input Modules HART 304
16.2.3.4 4 Channel Analog Input Modules 305
16.2.3.5 8 Channel Analog Input Modules 306
16.2.3.6 3-Phase Power Measurement Module 307
16.2.4 Analog Output Modules 309
16.2.4.1 2 Channel Analog Output Modules 309
16.2.4.2 4 Channel Analog Output Modules 309
16.2.5 Specialty Modules 310
16.2.5.1 Counter Modules 310
16.2.5.2 Pulse Width Modules 313
16.2.5.3 Serial Interface Modules with Alternative Data Format 313
16.2.5.4 Serial Interface Modules with Standard Data Format 314
16.2.5.5 Serial Interface Modules 314
16.2.5.6 Data Exchange Module 315
16.2.5.7 SSI Transmitter Interface Modules 315
16.2.5.8 Incremental Encoder Interface Modules 316
16.2.5.9 DC-Drive Controller 318
16.2.5.10 Stepper Controller 319
16.2.5.11 RTC Module 320
16.2.5.12 DALI Multi-Master Module 320
16.2.5.13 LON® FTT Module 324
16.2.5.14 EnOcean Radio Receiver 324
16.2.5.15 MP Bus Master Module 325
16.2.5.16 *Bluetooth*® RF-Transceiver 325
16.2.5.17 Vibration Velocity/Bearing Condition Monitoring VIB I/O 326
16.2.5.18 KNX/EIB/TP1 Module 327
16.2.5.19 AS-interface Master Module 327
16.2.6 System Modules 329
16.2.6.1 System Modules with Diagnostics 329
16.2.6.2 Filter Module 329
16.2.6.3 Binary Space Module 329

List of Figures 331

List of Tables 333

1 Notes about this Documentation



Note

Always retain this documentation!
This documentation is part of the product. Therefore, retain the documentation during the entire service life of the product. Pass on the documentation to any subsequent user. In addition, ensure that any supplement to this documentation is included, if necessary.

1.1 Validity of this Documentation

This documentation is only applicable to the “PFC100; 2ETH; ECO” controller (750-8100).

This documentation is only applicable from FW Version 03.10.08(22).

1.2 Copyright

This Manual, including all figures and illustrations, is copyright-protected. Any further use of this Manual by third parties that violate pertinent copyright provisions is prohibited. Reproduction, translation, electronic and phototechnical filing/archiving (e.g., photocopying) as well as any amendments require the written consent of WAGO GmbH & Co. KG, Minden, Germany. Non-observance will involve the right to assert damage claims.

1.3 Property rights

Third-party trademarks are used in this documentation. This section contains the trademarks used. The “®” and “TM” symbols are omitted hereinafter.

- Adobe® and Acrobat® are registered trademarks of Adobe Systems Inc.
- Android™ is a trademark of Google LLC.
- Apple, the Apple logo, iPhone, iPad and iPod touch are registered trademarks of Apple Inc. registered in the USA and other countries. “App Store” is a service mark of Apple Inc.
- AS-Interface® is a registered trademark of the AS-International Association e.V.
- BACnet® is a registered trademark of the American Society of Heating, Refrigerating and Air Conditioning Engineers, Inc. (ASHRAE).
- *Bluetooth*® is a registered trademark of Bluetooth SIG, Inc.
- CiA® and CANopen® are registered trademarks of CAN in AUTOMATION – International Users and Manufacturers Group e.V.
- CODESYS is a registered trademark of CODESYS Development GmbH.
- DALI is a registered trademark of the Digital Illumination Interface Alliance (DiiA).
- EtherCAT® is a registered trademark and patented technology licensed by Beckhoff Automation GmbH, Germany.
- ETHERNET/IP™ is a registered trademark of the Open DeviceNet Vendor Association, Inc (ODVA).
- EnOcean® is a registered trademark of EnOcean GmbH.
- Google Play™ is a registered trademark of Google Inc.
- IO-Link is a registered trademark of PROFIBUS Nutzerorganisation e.V.
- KNX® is a registered trademark of the KNX Association cvba.
- Linux® is a registered trademark of Linus Torvalds.
- LON® is a registered trademark of the Echelon Corporation.
- Modbus® is a registered trademark of Schneider Electric, licensed for Modbus Organization, Inc.
- OPC UA is a registered trademark of the OPC Foundation.

- PROFIBUS® is a registered trademark of the PROFIBUS Nutzerorganisation e.V. (PNO).
- PROFINET® is a registered trademark of the PROFIBUS Nutzerorganisation e.V. (PNO).
- QR Code is a registered trademark of DENSO WAVE INCORPORATED.
- Subversion® is a trademark of the Apache Software Foundation.
- Windows® is a registered trademark of Microsoft Corporation.

1.4 Symbols

DANGER

Personal Injury!
Indicates a high-risk, imminently hazardous situation which, if not avoided, will result in death or serious injury.



DANGER

Personal Injury Caused by Electric Current!
Indicates a high-risk, imminently hazardous situation which, if not avoided, will result in death or serious injury.

WARNING

Personal Injury!
Indicates a moderate-risk, potentially hazardous situation which, if not avoided, could result in death or serious injury.

CAUTION

Personal Injury!
Indicates a low-risk, potentially hazardous situation which, if not avoided, may result in minor or moderate injury.

NOTICE

Damage to Property!
Indicates a potentially hazardous situation which, if not avoided, may result in damage to property.



NOTICE

Damage to Property Caused by Electrostatic Discharge (ESD)!
Indicates a potentially hazardous situation which, if not avoided, may result in damage to property.



Note

Important Note!
Indicates a potential malfunction which, if not avoided, however, will not result in damage to property.



Information

Additional Information:
Refers to additional information which is not an integral part of this documentation (e.g., the Internet).

1.5 Number Notation

Table 1: Number Notation

Number Code	Example	Note
Decimal	100	Normal notation
Hexadecimal	0x64	C notation
Binary	'100' '0110.0100'	In quotation marks, nibble separated with dots (.)

1.6 Font Conventions

Table 2: Font Conventions

Font Type	Indicates
italic	Names of paths and data files are marked in italic-type. e.g.: *C:\Program Files\WAGO Software*
Menu	Menu items are marked in bold letters. e.g.: **Save**
>	A greater-than sign between two names means the selection of a menu item from a menu. e.g.: **File** > **New**
Input	Designation of input or optional fields are marked in bold letters, e.g.: **Start of measurement range**
“Value”	Input or selective values are marked in inverted commas. e.g.: Enter the value “4 mA” under **Start of measurement range**.
[Button]	Pushbuttons in dialog boxes are marked with bold letters in square brackets. e.g.: **[Input]**
[Key]	Keys are marked with bold letters in square brackets. e.g.: **[F5]**

2 Important Notes

This section includes an overall summary of the most important safety requirements and notes that are mentioned in each individual section. To protect your health and prevent damage to devices as well, it is imperative to read and carefully follow the safety guidelines.

2.1 Legal Bases

2.1.1 Subject to Changes

WAGO GmbH & Co. KG reserves the right to provide for any alterations or modifications. WAGO GmbH & Co. KG owns all rights arising from the granting of patents or from the legal protection of utility patents. Third-party products are always mentioned without any reference to patent rights. Thus, the existence of such rights cannot be excluded.

2.1.2 Personnel Qualifications

All sequences implemented on WAGO I/O System 750 devices may only be carried out by electrical specialists with sufficient knowledge in automation. The specialists must be familiar with the current norms and guidelines for the devices and automated environments.

All changes to the coupler or controller should always be carried out by qualified personnel with sufficient skills in PLC programming.

2.1.3 Use of the 750 Series in Compliance with Underlying Provisions

Fieldbus couplers, controllers and I/O modules found in the modular WAGO I/O System 750 receive digital and analog signals from sensors and transmit them to actuators or higher-level control systems. Using controllers, the signals can also be (pre-) processed.

The devices fulfill the requirements of protection type IP20 and are designed for use in dry interior spaces. There is protection against finger injury and solid impurities ≥ 12.5 mm diameter is assured; protection against water damage is not ensured.
The devices represent open-type devices. They may only be installed in enclosures (tool-secured enclosures or operating rooms) which fulfil the listed requirements specified in the safety instructions in chapter “Safety Advice (Precautions)”. Use without additional protective measures in environments within which dust, corrosive fumes, gases or ionized radiation can occur is considered improper use.

Operating the WAGO I/O System 750 devices in home applications without further measures is only permitted if they meet the emission limits (emissions of interference) according to EN 61000-6-3. You will find the relevant information in

the section “Device Description” > “Standards and Guidelines” in the manual for the used device.

Appropriate housing (per 2014/34/EU) is required when operating the WAGO I/O System 750 in hazardous environments. Please observe the installation regulations! Please note that a prototype test certificate must be obtained that confirms the correct installation of the system in a housing or switch cabinet.

The implementation of safety functions such as EMERGENCY STOP or safety door monitoring must only be performed by the F I/O modules within the modular WAGO I/O System 750. Only these safe F I/O modules ensure functional safety in accordance with the latest international standards. WAGO's interference-free output modules can be controlled by the safety function.

2.1.4 Technical Condition of Specified Devices

The devices to be supplied ex works are equipped with hardware and software configurations, which meet the individual application requirements. These modules contain no parts that can be serviced or repaired by the user. The following actions will result in the exclusion of liability on the part of WAGO GmbH & Co. KG:

- Repairs,
- Changes to the hardware or software that are not described in the operating instructions,
- Improper use of the components.

Further details are given in the contractual agreements. Please send your request for modified and new hardware or software configurations directly to WAGO GmbH & Co. KG.

2.2 Safety Advice (Precautions)

For installing and operating purposes of the relevant device to your system the following safety precautions shall be observed:



DANGER

Do not work on devices while energized!
All power sources to the device shall be switched off prior to performing any installation, repair or maintenance work.

DANGER

Install device in a suitable enclosure!
The device is an open system. Install the device in a suitable enclosure. This enclosure must:

- Guarantee that the max. permissible degree of pollution is not exceeded.
- Offer adequate protection against contact.
- Prevent fire from spreading outside of the enclosure.
- Offer adequate protection against UV irradiation.
- Guarantee mechanical stability
- Restrict access to authorized personnel and may only be opened with tools



DANGER

Ensure disconnect and overcurrent protection!
The device is intended for installation in automation technology systems. Disconnect protection is not integrated. Connected systems must be protected by a fuse.
Provide suitable disconnect and overcurrent protection on the system side!

DANGER

Ensure a standard connection!
To minimize any hazardous situations resulting in personal injury or to avoid failures in your system, the data and power supply lines shall be installed according to standards, with careful attention given to ensuring the correct terminal assignment. Always adhere to the EMC directives applicable to your application.



⚠ CAUTION

Inadequate wire cross sections can cause temperature increases!
To avoid increasing thermal risks, only use conductor cross-sections sufficient for the required maximum load current. The conductor cross-sections specified in the technical data refer exclusively to the mechanical connection capacity of the clamping points.

NOTICE

Do not use in telecommunication circuits!
Only use devices equipped with ETHERNET or RJ-45 connectors in LANs. Never connect these devices with telecommunication networks.

NOTICE

Ensure proper contact with the DIN-rail!
Proper electrical contact between the DIN-rail and device is necessary to maintain the EMC characteristics and function of the device.

NOTICE

Replace defective or damaged devices!
Replace defective or damaged device/module (e.g., in the event of deformed contacts).

NOTICE

Protect the components against materials having seeping and insulating properties!
The components are not resistant to materials having seeping and insulating properties such as: aerosols, silicones and triglycerides (found in some hand creams). If you cannot exclude that such materials will appear in the component environment, then install the components in an enclosure being resistant to the above-mentioned materials. Clean tools and materials are imperative for handling devices/modules.

NOTICE

Clean only with permitted materials!
Clean housing and soiled contacts with propanol.

NOTICE

Do not use any contact spray!
Do not use any contact spray. The spray may impair contact area functionality in connection with contamination.

NOTICE

Do not reverse the polarity of connection lines!
Avoid reverse polarity of data and power supply lines, as this may damage the devices involved.

NOTICE



Avoid electrostatic discharge!
The devices are equipped with electronic components that may be destroyed by electrostatic discharge when touched. Please observe the safety precautions against electrostatic discharge per DIN EN 61340-5-1/-3. When handling the devices, please ensure that environmental factors (personnel, work space and packaging) are properly grounded.

2.3 Licensing Terms of the Software Package Used

The firmware for the “PFC100; 2ETH; ECO” controller (750-8100) contains open-source software.

The licence conditions of the software packages are stored in the controller in text form. They can be accessed via the WBM page “Legal Information” > “Open Source Software.”
You can obtain the source code with licensing terms of the open-source software from WAGO GmbH & Co. KG on request. Send your request to support@wago.com with the subject “Controller Board Support Package.”

2.4 Special Use Conditions for ETHERNET Devices

If not otherwise specified, ETHERNET devices are intended for use on local networks. Please note the following when using ETHERNET devices in your system:

- Do not connect control components and control networks directly to an open network such as the Internet or an office network. WAGO recommends putting control components and control networks behind a firewall.
- In the control components (e.g., for WAGO I/-CHECK and CODESYS) close all ports and services not required by your application to minimize the risk of cyber attacks and to enhance cyber security.
  Only open ports and services during commissioning and/or configuration.
- Limit physical and electronic access to all automation components to authorized personnel only.
- Change the default passwords before first use! This will reduce the risk of unauthorized access to your system.
- Regularly change the passwords used! This will reduce the risk of unauthorized access to your system.
- If remote access to control components and control networks is required, use a Virtual Private Network (VPN).
- Regularly perform threat analyses. You can check whether the measures taken meet your security requirements.
- Use “defense-in-depth” mechanisms in your system's security configuration to restrict the access to and control of individual products and networks.
- Please note the risks of using cloud services!
  If you use third-party cloud services, sensitive data is transferred to the cloud service provider at one's own responsibility. External access may result in manipulated data and/or unwanted control commands affecting the

performance of your control system.
Use encryption methods to protect your data and observe the information provided by the Federal Office for Information Security – “Cloud: Risks and Security Tips”.
Observe comparable publications of the competent, public institutions of your country.

3 Overview

The controller 750-8100(PFC100; 2ETH; ECO) is an automation device that can perform control tasks of a PLC. It is suitable for mounting on a DIN rail and stands out on account of its various interfaces.

This controller can be used for applications in mechanical and systems engineering, in the processing industry and in building technology.

You can connect all available I/O modules of the WAGO-I/O-SYSTEM 750 (750 and 753 Series) to the controller, enabling it to internally process analog and digital signals from the automation environment, or to supply these signals to other devices via one of the available interfaces.

Automation tasks can be executed in all IEC 61131-3-compatible languages with the ***e!****COCKPIT* programming system.
The implementation of the task processing in the runtime system for Linux® has been optimized with real-time extensions in order to provide maximum performance for automation tasks. Web visualization is also provided as visualization in addition to the development environment.

For IEC-61131-3 programming in CODESYS applications, the controller provides 10 MB of program and data memory (dynamically distributed) and 64 kB of retentive memory (retain and flag variables) in an integrated NVRAM.

The controller has a slot for an SD card. The SD card can be used to transfer device parameters, boot projects and other files from one controller to another. The SD card can be accessed via FTP as an additional drive.



Note

Memory card is not included in the scope of delivery!
Note, the controller is delivered without memory card.
To use a memory card, you must order one separately. The controller can also be operated without memory card expansion, the use of a memory card is optional.



Note

Only use recommended memory cards!
Use only the microSD memory card available from WAGO (item No. 758-879/000-3102) as it is suitable for industrial applications subjected to environmental extremes and for use in this device.
Compatibility with other commercially available storage media cannot be guaranteed.

Two ETHERNET interfaces and the integrated, configurable switch enable wiring in all necessary configurations with one common network where both ports share

a common IP address or with two separate networks where each port has its own IP address.

The physical interfaces (ports) are assigned via logical bridges and can be e.g., configured via the WBM.

Both of these interfaces support:

- 10BASE-T / 100BASE-TX
- Full/Half duplex
- Autonegotiation
- Auto-MDI(X) (automatic uplink and crossover switching)

The following fieldbus circuits are implemented for exchange of process data:

- Modbus TCP Master/Slave
- Modbus UDP Master/Slave

In the controller, all input signals from the sensors are combined. After connecting the controller, all of the I/O modules on the bus node are detected and a local process image is created from these. Analog and specialty module data is sent via words and/or bytes; digital data is sent bit by bit.



Note

No direct access from fieldbus to the process image for I/O modules!
Any data that is required from the I/O module process image must be explicitly mapped in the CODESYS program to the data in the fieldbus process image and vice versa! Direct access is not possible!

e!*COCKPIT* makes configuring the fieldbus possible.

A Web-based management system (WBM) is also available as a configuration aid. This system includes various dynamic HTML pages from which, among other things, information about configuration and the status of the controller can be called up. The WBM is already stored in the device and is presented and operated using a web browser. You can also save your own HTML pages in the implemented file system, or call up programs directly.

In the controller's initial state, the installed firmware is based on Linux®, with special real-time extensions of the RT-Preempt patch. In addition, the following application programs are also installed on the controller, along with a number of different auxiliary programs:

- a SNMP server/client
- a FTP server, a FTPS server (explicit connections only)

- a SSH server/client
- a Web server
- a NTP client
- a BootP and DHCP client
- a DHCP server
- a DNS server
- an ***e!****RUNTIME* Runtime Environment

Based on IEC-61131-3 programming, data processing takes place on site in the controller. The logical process results can be output directly to the actuators or transmitted via a connected fieldbus to the higher level controller.

4 Properties

4.1 Hardware Description

4.1.1 View

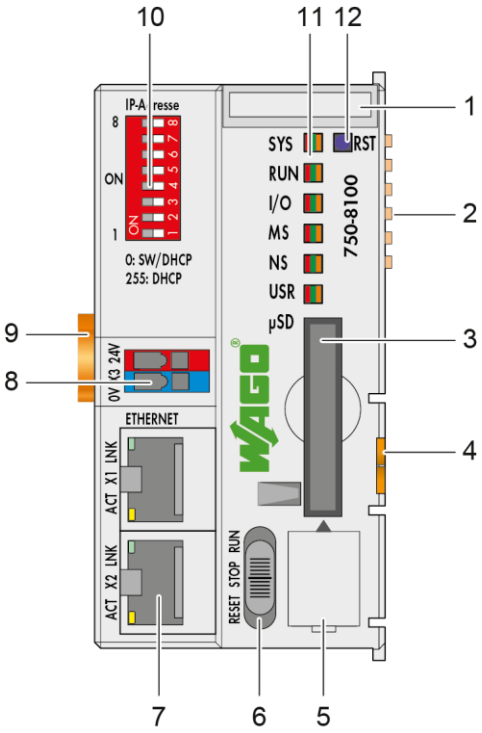


Figure 1: View

Table 3: Legend for Figure “View”

Item	Description	See section
1	Marking options (Mini WSB)	---
2	Data contacts	“Connectors” > “Data Contacts/Local Bus”
3	Slot for memory card	“Slot for Memory Card”
4	Releasing strap	“Mounting” > “Inserting Devices” “Removal” > “Removing Devices”
5	Service Interface (behind the flap)	“Connectors” > “Service Interface”
6	Mode selector switch	“Operating elements” > “Operating Mode Switch”
7	ETHERNET connectors – X1, X2	“Connectors” > “Network connectors”

8	Safe locking feature	“Mounting” > “Inserting Devices” “Removal” > “Removing Devices”
9	CAGE CLAMP® connectors for power supply	“Connectors” > “CAGE CLAMP® connectors”
10	Address selection switch	“Operating Elements” > “Address Selection Switch”
11	LED indicators – system	“Display Elements” > “Fieldbus/System Indicating Elements”
12	Reset button (in hole)	“Operating Elements” > “Reset Button”

4.1.2 Labeling

The front labeling includes:
- Device designation
- Name of the display elements, connections and control elements
- Serial number with hardware and firmware version

The side labeling includes:
- Manufacturer's identification
- Connector pin assignment
- Serial number
- Approval information

4.1.2.1 Production Code

The serial number indicates the delivery status directly after production.

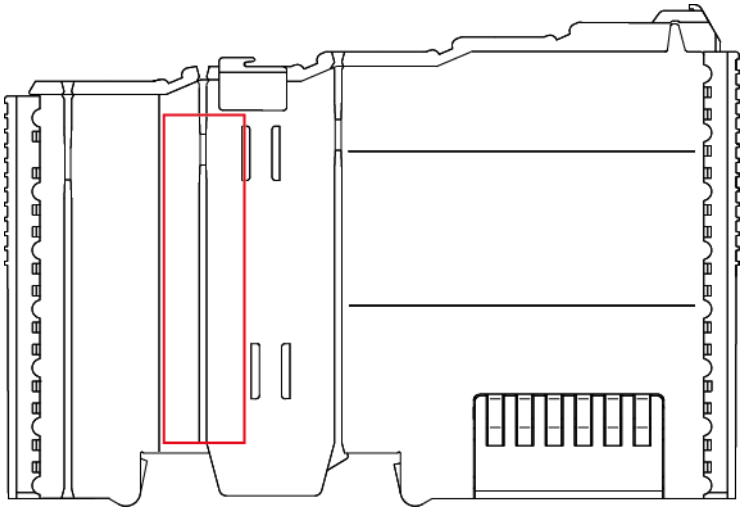


Figure 2: Marking Area for Serial Numbers

There are two serial numbers in two rows in the side marking. They are left of the release tab. The first 10 positions in the longer row of the serial numbers contain version and date identifications.

Example structure of the rows: 0114010101…

01	**14**	**01**	**01**	**01**	**(additional positions)**
WW	**YY**	**FW --**	**HW**	**FL**	**-**
Calendar week	Year	Firmware version	Hardware version	Firmware loader version	Internal information

The row order can vary depending on the production year, only the longer row is relevant. The back part of this and the shorter row contain internal administration information from the manufacturer.

4.1.3 Connectors

4.1.3.1 Service Interface

The service interface is located behind the flap.

The Service interface is used for communication with WAGO-I/O-*CHECK* and “WAGO Ethernet Settings”.

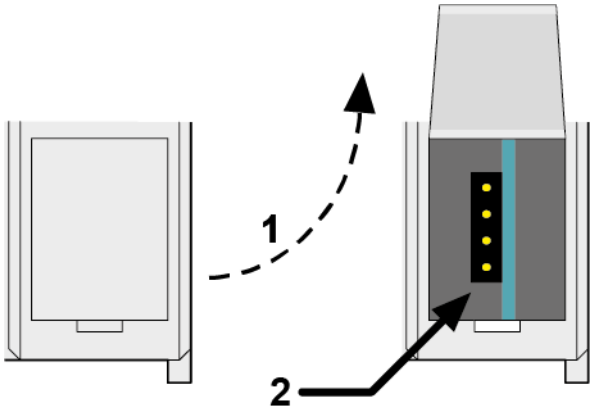


Figure 3: Service Interface (Closed and Open Flap)

Table 4: Service Interface

Number	Description
1	Open flap
2	Service interface

NOTICE

Device must be de-energized!
To prevent damage to the device, unplug and plug in the communication cable only when the device is de-energized!

The connection to the 4-pin header under the cover flap can be realized via the communication cables with the item numbers750-920 and 750-923 or via the WAGO radio adapter with the item number 750-921.

4.1.3.2 Network Connectors

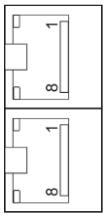


Figure 4: Network Connections – X1, X2

Table 5: Legend for Figure “Network Connections – X1, X2”

Contact	Signal	Description
1	TD +	Transmit Data +
2	TD −	Transmit Data −
3	RD +	Receive Data +
4	NC	Not assigned
5	NC	Not assigned
6	RD −	Receive Data −
7	NC	Not assigned
8	NC	Not assigned

4.1.3.3 Wiring Level

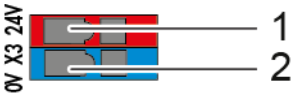


Figure 5: CAGE CLAMP® Connections (X3)

Table 6: Legend for Figure “CAGE CLAMP® Connections (X3)”

Position	Designation	Description
1	24 V	System power supply voltage +24 V
2	0 V	System power supply voltage 0 V

4.1.4 System Contacts

4.1.4.1 Data Contacts

Communication between the controller and the I/O modules and system power supply for the I/O modules is provided via the local bus, which consists of 6 data contacts designed as self-cleaning gold spring contacts.

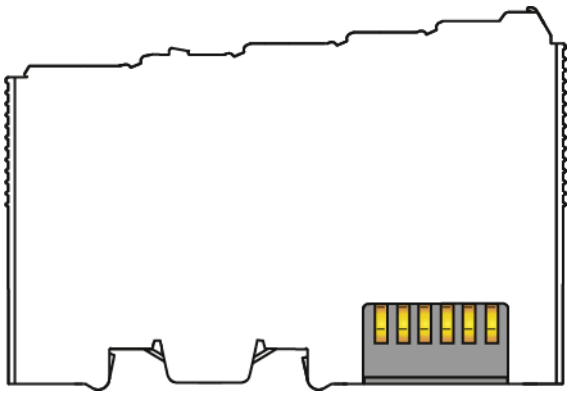


Figure 6: Data Contacts

NOTICE

Do not place the I/O modules on the gold spring contacts!
Do not place the I/O modules on the gold spring contacts in order to avoid soiling or scratching!

NOTICE



Pay attention to potential equalization from the environment!
The devices are equipped with electronic components that may be destroyed by electrostatic discharge. When handling the devices, please ensure that environmental factors (personnel, work space and packaging) are properly equalized. Do not touch any conducting parts, e.g., data contacts.

NOTICE

Do not exceed the maximum total current for I/O modules (5 VDC) via data contacts!
The maximum permissible total current for internal system supply of the I/O modules may not be exceeded. The permissible total current is specified in the technical data of the head station and power supply. The data contacts for internal system supply can be damaged and the permissible operating temperature can be exceeded by higher values.
When configuring the system, do not exceed the permissible total current. If there is a higher power requirement, you must use an additional supply to provide the system voltage (5 VDC)!

4.1.5 Display Elements

4.1.5.1 System/Fieldbus LEDs



Figure 7: Indicating elements for fieldbus/system

Table 7: Legend for Figure “Fieldbus/System Indicating Elements”

Designation	Color	Description
SYS	Red/Green/ Orange/Off	System status
RUN	Red/Green/ Orange/Off	PLC program status
I/O	Red/Green/ Orange/Off	Local bus status
MS	Red/Green/ Orange/Off	Module status
NS	Red/Green/ Orange/Off	Without function
USR	Red/Green/ Orange/Off	User LED, programmable using function blocks from the WAGO libraries to control the LEDs

4.1.5.2 Network Connector LEDs

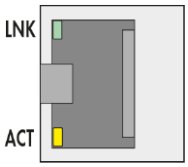


Figure 8: Indicating Elements, RJ-45 Jacks

Table 8: Legend for Figure “Indicating Elements, RJ-45 Jacks”

Designation	Color	Description
LNK	Green/Off	ETHERNET connection status
ACT	Yellow/Off	ETHERNET data exchange

4.1.5.3 Memory Card Slot LED

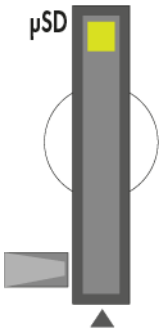


Figure 9: Indicating Elements, Memory Card Slot

Table 9: Legend for Figure “Indicating Elements, Memory Card Slot”

Description	Color	Description
µSD	Yellow/Off	Memory card status

4.1.6 Operating Elements

4.1.6.1 Address Selection Switch

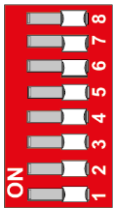


Figure 10: Address Selection Switch (here setting “0”)

Table 10: Significance of the Address Values of the Address Selection Switch

Address value	Explanation
0	The IP parameters are configured via the settings in the Web-Based Management (WBM), Console-Based Management (CBM) or by the factory settings.
1 … 254	A fixed IP address is assigned. The IP address consists of the network address and the set address value. The network address can be configured from the CBM or WBM and is 192.168.1 by default.
255	The DHCP protocol is used to configure the IP parameters.

4.1.6.2 Operating Mode Switch

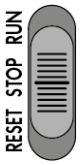


Figure 11: Mode Selector Switch

Table 11: Mode Selector Switch

Position	Actuation	Function
RUN	Latching	**Normal operation** ***e!****RUNTIME* applications running.
STOP	Latching	**Stop** All ***e!****RUNTIME* applications have stopped.
RESET	Spring-return	**Reset warm start** or **Reset cold start** (depending on length of actuation, see Section “Starting” > “Initiating Reset Functions”)

Other functions can also be initiated using the reset button.

4.1.6.3 Reset Button

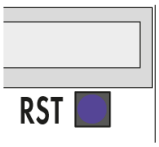


Figure 12: Reset Button

The Reset button is installed behind drilling to prevent operating errors. It is a shortstroke button with a low actuating force of 1.1 N … 2.1 N (110 gf … 210 gf). The button can be actuated using a suitable object (e.g., pen).

You can initiate different functions using the Reset button depending on the position of the mode selector:

- Temporarily set a fixed IP address (“Fixed IP Address” mode, see section “Commissioning” > “Setting an IP Address” > “Temporarily Setting a Fixed IP Address”)
- Perform a software reset (restart, see section “Commissioning” > “Initiating Reset Functions” > “Software Reset”)
- Restore factory setting (factory reset, see section “Service” > “Firmware Changes” > “Factory Reset”)

4.2 Slot for Memory Card

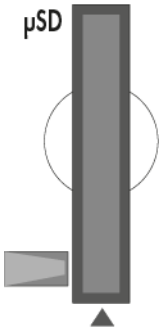


Figure 13: MicroSD Card Slot

The microSD card is locked in the enclosure by a push/push mechanism.
Inserting and removing the card is described in the Section “Service” > “Inserting and Removing the Memory Card”.
The microSD card is protected by a cover flap, which can also be sealed.

The microSD card is locked in the enclosure by a push/push mechanism.
Inserting and removing the card is described in the Section “Service” > “Inserting and Removing the Memory Card”.
The microSD card is protected by a cover flap, which can also be sealed.

Note

Memory card is not included in the scope of delivery!
Note, the controller is delivered without memory card.
To use a memory card, you must order one separately. The controller can also be operated without memory card expansion, the use of a memory card is optional.

Note

Only use recommended memory cards!
Use only the microSD memory card available from WAGO (item No. 758-879/000-3102) as it is suitable for industrial applications subjected to environmental extremes and for use in this device.
Compatibility with other commercially available storage media cannot be guaranteed.

4.3 Schematic Diagram

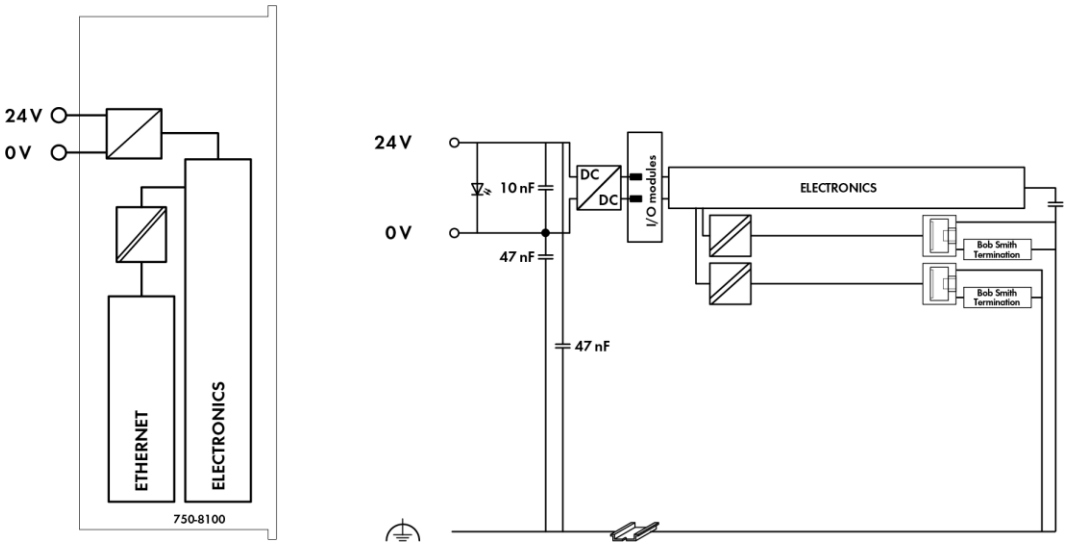


Figure 14: Schematic switching diagram

4.4 Technical Data

4.4.1 Mechanical Data

Table 12: Technical Data – Mechanical Data

Width	49.5 mm / 1.949 inch
Height	96.8 mm / 3.811 inch
Depth	71.9 mm / 2.831 inch
Depth from upper edge of DIN-rail	64.7 mm / 2.547 inch
Weight	112 g

4.4.2 System Data

Table 13: Technical Data – System Data

CPU	Cortex A8, 600 MHz
Operating System	Real-time Linux® 4.9.47-rt37 (with RT Preemption Patch)
MicroSD card slot	Push-push mechanism, sealable cover lid
Type of memory card	microSD up to 32 Gbytes (All guaranteed properties are valid only in connection with the WAGO 758-879/000-3102 memory card.)

4.4.3 Power Supply

Table 14: Technical Data – Power Supply

Power supply	24 VDC (-25 % … +30 %)
Max. input current (24 V)	550 mA
Power failure time acc. IEC 61131-2	Depending on external buffering
Total current for I/O modules (5V)	700 mA
Isolation	500 V system/supply



Note

Buffer for system power supply!
The system power supply and, if necessary, the field supply must be buffered to bridge power outages.
As the power demand depends on the respective node configuration, buffering is not implemented internally.
To achieve power outages of 1 ms to 10 ms according to IEC61131-2, determine the buffering appropriate for your node configuration and structure it as an external circuit.

4.4.4 Clock

Table 15: Technical Data – Clock

Drift - system clock (25 °C)	20 ppm
Drift - RTC (25 °C)	3 ppm
Buffer time RTC (25 °C)	7 days

4.4.5 Programming

Table 16: Technical Data – Programming

Programming	***e!****COCKPIT*
IEC 61131-3	LD, FBD (CFC), ST, FC
Program and data memory	10 MB (dynamically distributed)
Non-volatile memory (NVRAM, retain + flag)	64 Kbytes

4.4.6 Local Bus

Table 17: Technical Data – Local Bus

Number of I/O modules (per node)	64
with bus extension	250
Input and output process image (max.)	Not specified

4.4.7 ETHERNET

Table 18: Technical Data – ETHERNET

ETHERNET	2 x RJ-45 (switched or separated mode)
Transmission medium	Twisted Pair S-UTP, 100 Ω, Cat 5, 100 m maximum cable length
Baud rate	10/100 Mbit/s; 10Base-T/100Base-TX
Protocols	DHCP, DNS, SNTP, FTP, FTPS (only explicit connections), SNMP, HTTP, HTTPS, SSH, Modbus (TCP, UDP)
Modbus – input and output process image max.	32000 words

Note

No direct access from fieldbus to the process image for I/O modules!
Any data that is required from the I/O module process image must be explicitly mapped in the CODESYS program to the data in the fieldbus process image and vice versa! Direct access is not possible!

4.4.8 Connection Type

Table 19: Technical Data – Field Wiring

Connection technology	CAGE CLAMP®
Conductor cross-section	0.08 mm² … 2.5 mm², AWG 28 … 14
Strip length	8 mm … 9 mm / 0.33 in

Table 20: Technical Data – Data Contacts

Data contacts	Slide contact, hard gold plated, self-cleaning

4.4.9 Climatic Environmental Conditions

Table 21: Technical Data – Climatic Environmental Conditions

Surrounding air temperature, operation	0 °C … 55 °C
Surrounding air temperature, storage	−25 °C … +85 °C
Relative humidity without condensation	5 % … 95 % without condensation
Operating altitude	0 … 2000 m
Pollution degree	2
Overvoltage category	II
Protection type	IP20
Resistance to harmful substances	Acc. to IEC 60068-2-42 and IEC 60068-2-43
Maximum pollutant concentration at relative humidity < 75 %	$SO_2 \leq 25$ ppm $H_2S \leq 10$ ppm
Special conditions	• Ensure that additional measures for components are taken, which are used in an environment involving: – dust, caustic vapors or gases – ionizing radiation • The permissible temperature range of the connecting cable must be dimensioned based on the mounting position and current intensity, as the temperature of the terminal connection can be up to 25 °K above the maximum expected surrounding air temperature (at 10 A).

4.5 Approvals

For current approvals, please go to: www.wago.com/<Item number>.

The following approvals have been granted to the “PFC100; 2ETH; ECO” controller (750-8100):

Conformity Marking

UL508

The following Ex approvals have been granted to the “PFC100; 2ETH; ECO” controller (750-8100):

Hazardous Locations	UL 121201 for Use in Hazardous Locations Cl I Div 2

TÜV 14 ATEX 148929 X

II 3 G Ex nA IIC T4 Gc

IECEx TUN 14.0035 X

Ex nA IIC T4 Gc

2020312310000213

Ex nA IIC T4 Gc

EAC RU C-DE.AM02.B.00163/19

2Ex e IIC T4 Gc X

The following ship approvals have been granted to the “PFC100; 2ETH; ECO” controller (750-8100):

ABS (American Bureau of Shipping)

BV (Bureau Veritas)

DNV GL
[Temperature: B, Humidity: B, Vibration: B, EMC: B, Enclosure: (*)]
(*) Required protection according to the rules shall be provided upon installation on board.

LR (Lloyd’s Register) Env. 1, 2, 3, 4

PRS (Polski Rejestr Statków)

RINA (Registro Italiano Navale)

Information

For more information about the ship approvals:
Note the “Supplementary Power Supply Regulations” section for the ship approvals.

4.6 Standards and Guidelines

The “PFC100; 2ETH; ECO” controller (750-8100) fulfills the following EMC standards:

EMC CE-Immunity to interference	EN 61000-6-2
EMC CE-Emission of interference	EN 61000-6-3

5 Function Description

5.1 Network

5.1.1 Interface Configuration

The X1 and X2 network interfaces of the controller are connected with an integrated configurable 3-port switch, in which the third port is connected to the CPU.

The two interfaces and configurable switch enable wiring for:

- One common network where both ports share a common IP address.
- Two separate networks where each port has its own IP address.

The physical interfaces (ports) are assigned via logical bridges and can be e.g., configured via the WBM.

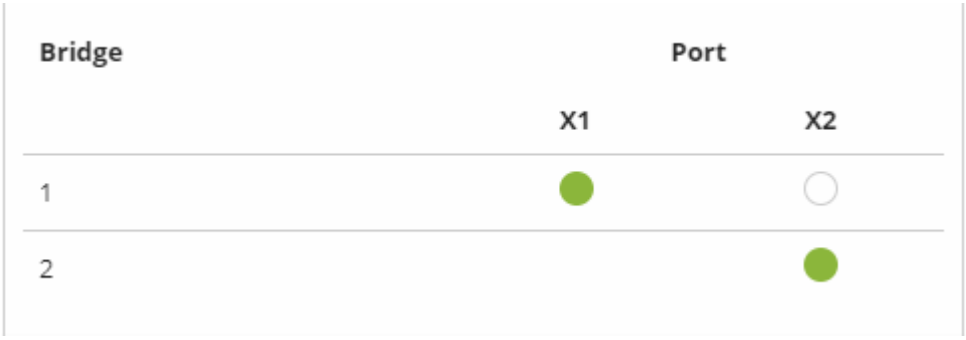


Figure 15: Example of Interface Assignment via WBM

5.1.1.1 Operation in Switch Mode

For operation in Switch mode, the TCP/IP settings such as the IP address or subnet mask apply to both X1 and X2.

When switching to Switch mode, the X1 settings are applied as a new common configuration for X1 and X2.
The device is then no longer accessible via the IP address previously set for X2. This must be taken into account for CODESYS applications that use X2 for communication.

5.1.1.2 Operation with Separate Network Interfaces

When operating with separate network interfaces, both ETHERNET interfaces can be configured and used separately.
Note that the two interfaces still have the same MAC address. Therefore, they must not be operated in the same network segment.

When switching to operating with separate interfaces, interface X2 is initialized with the setting values last valid for it. The connections on the X1 interface persist.

When operating with separate interfaces and fixed IP address, the device can still be accessed via the interface X2 via the regular IP address.

5.1.2 Network Security

5.1.2.1 Users and Passwords

Several groups of users are provided in the controller which can be used for various services.

Default passwords are set for all users. We strongly recommend changing these passwords on startup!

Note

Change passwords
Default passwords are documented in these instructions and therefore do not offer adequate protection! Change the passwords to meet your particular needs.

5.1.2.1.1 Services and Users

All password-protected services and their associated users are listed in the following table.

Table 22: Services and Users

Service	Users			
	Linux			SNMP
	root	admin	user	
Web Based Management (WBM)	X	X	X	
Linux console	X	X	X	
Console Based Management (CBM)	X			
CODESYS		X		
Telnet	X	X	X	
FTP	X	X	X	
FTPS	X	X	X	
SSH	X	X	X	
SNMP				X

5.1.2.1.2 WBM User Group

The WBM uses part of the Linux users.

Table 23: WBM Users

Users	Permissions	Default Password
root	All (administrator)	wago
admin	All (administrator)	wago
user	Supported to a limited extent	user
guest	Display only	---



Note

General Rights of WBM Users

The WBM users “root”, “admin” and “user” have rights beyond the WBM to configure the system and install software.



Note

Change passwords

Default passwords are documented in these instructions and therefore do not offer adequate protection! Change the passwords to meet your particular needs.

More information is available in the Section “WBM User Administration”.

5.1.2.1.3 Linux User Group

The Linux user group includes the actual users of the operating system, which is likewise used by most services.

Table 24: Linux Users

User	Special Feature	Home Directory	Default Password
root	Super user	/root	wago
admin	CODESYS user	/home/admin	wago
user	Normal user	/home/user	user

You can configure passwords for these users via a terminal connection.



Note

Change passwords
Default passwords are documented in these instructions and therefore do not offer adequate protection! Change the passwords to meet your particular needs.



Note

Note password length!
For CODESYS, the password length must be greater than or equal to 1 character and less than 60 characters!

5.1.2.1.4 SNMP User Group

The SNMP service manages its own users. In its initial state, no users are stored in the system.

5.1.2.2 Web Protocols for WBM Access

The HTTP and HTTPS web protocols can be used to access the WBM pages for the controller. HTTPS is preferred because it uses the SSL/TLS protocol. The SSL/TLS protocol ensures secure communication through encryption and authentication

The default setting for the controller allows strong encryption, but uses only simple authentication methods. As authentication for any secure communication channel plays a central role, it is strongly recommended that you use secure authentication. The security certificate saved on the controller is the basis for authentication. The default location for the security certificate is: /etc/lighttpd/https-cert.pem

As delivered, the controller uses a generic security certificate based on x509. To allow secure authentication, you must replace the generic security certificate with a security certificate specific for the individual device.

5.1.2.2.1 TLS Encryption

When an HTTPS connection is established, the Web browser and Webserver negotiate what TLS version and what cryptographic method are to be used.

The “TLS Configuration” group of the WBM page “Security” can be used to switch the cryptographic methods allowed for HTTPS and the TLS versions that can be used.

The settings “Strong” and “Standard” are possible.
If “Strong” is set, the Webserver only allows TLS Version 1.2 and strong algorithms.
Older software and older operating systems may not support TLS 1.2 and encryption algorithms.
If “Standard” is set, TLS 1.0, TLS 1.1 and TLS 1.2 are allowed, as well as cryptographic methods that are no longer considered secure.



Information

BSI Technical Guidelines TR-02102
The rules for the “Strong” setting are based on technical guidelines TR-02102 of the German Federal Office for Information Security.
You can find the guidelines on the Internet at: https://www.bsi.bund.de > “Publications” > “Technical Guidelines.”

Information

BSI Guidelines on Migration to TLS 1.2

The German Federal Office for Information Security guidelines on migration to TLS 1.2 contain “compatibility matrices” that show what software is comparable with TLS 1.2.

You can find the guidelines on the Internet at: https://www.bsi.bund.de > “Topics” > “Standards and Criteria” > “Minimum Standards“.

5.1.2.3 Root Certificates

For communication encrypted with TLS, root certificates are used to verify the authenticity of the communication partner.
A root certificate, which is signed by a certificate authority, serves to verify the validity of all certificates issued by this certificate authority.

The root certificates stored on the controller (root CA bundle) form the basis for authentication of services hosted on the Internet (e.g., email providers and cloud services).

The standard storage location for the root certificates is /etc/ssl/certs/ca-certificates.crt.

This file contains the certificates provided by Mozilla. A list of the included root certificates and their respective validity periods can be requested from the following address:

https://hg.mozilla.org/releases/mozilla-release/raw-file/79f079284141/security/nss/lib/ckfw/builtins/certdata.txt

The root certificates can be updated on the controller by updating the file /etc/ssl/certs/ca-certificates.crt (see section “Service” > “Updating Root Certificates”).

5.1.3 Network Configuration

5.1.3.1 Host Name/Domain Name

Without a host name configuration, the controller is assigned a default name which includes the last three values of the controller's MAC address, e.g., “PFCx00-A1A2A3.” This name is valid for as long as a host name was not configured, or host name was not supplied to the controller via DHCP (for configuration of the controller see Section “Startup” > “Configuring”). When the host name is set, a host name supplied by a DHCP response is immediately active and displaces the configured or default host name.

For multiple network interfaces with DHCP, the hostname is taken from the network interface (bridge or Wwan) with the highest priority. The priority is specified alphanumerically by the name of the network interface. Thus, Bridge1 has the highest priority, followed by Bridge2, Bridge3, ..., Wwan0.

If only the configured name is to be valid, the network administrator must adjust the configuration of the active DHCP server so that no host names are transferred in the DHCP response.

The default host name or the configured name is active again if the network interfaces are set to static IP addresses or if a host name is not received via the DHCP response.

A similar mechanism is used for a domain name as for the host name. The difference is that a default domain name is not set. As long as a domain name is not configured or supplied by DHCP, the domain name is empty.

5.1.3.2 Routing

As part of the TCP/IP configuration, the controller allows you to configure static routes, IP masquerading and port forwarding. Default gateways are configured via static routes, since default gateways are a special case of static routes.

A network station transmits to a gateway all network data packets for systems outside of its local network. This gateway is responsible for the appropriate routing of the data packets so that they reach the target system. To allow access to different target systems, it may be necessary to configure multiple gateways. This is configured by adding routing entries.
A routing entry consists of the following information:

- Destination address,
- Destination mask,
- Gateway address,
- Gateway metric.
- Interface

On the basis of the target system configuration, consisting of the destination address and destination mask, a decision is made about which gateway a network data packet should be forwarded to. The target system can be specified through an individual IP address or an IP address range. For a network data packet to forward, the routing entry with the most specific destination address and destination mask entries is always selected. The default gateway corresponds to the least specific routing entry. All network data packets such that no specific routing entry exists for their destination address and destination mask are sent to this default gateway.

Default gateway:
Default gateways, also called default routes, are always set in connection with the IP configuration.
Each default gateway has a metric that is unique among all default gateways. Bridge <n> has the metric 19+<n>.
A default gateway can also be defined via the routing configuration, e.g., to define an individual metric. The value “default” must be set for “Destination Address” and the value “0.0.0.0” for Destination Mask.

Route:
If an IP address or IP address range is entered in the “Destination Address” field, then all network data packets that are directed to the network address or network address range are sent to the gateway address corresponding to the entry. Alternatively, a bridge, a modem or a VPN interface can be specified in the “Interface” field, via which all data packets that are directed to the destination address are routed. Specifying an interface is optional. However, either a gateway address, an interface or both must be specified.

If the IP address of the gateway is outside the IP address space that the controller can reach, the associated route is not enabled. This also applies to routes in which an interface is specified, which e.g., is not enabled in the current bridge configuration.

A metric is assigned to each routing entry. If multiple routing entries are configured for the same destination address and destination mask, the metric specifies how the routing entries are prioritized. In this case, routing entries with a lower value for the metric are preferred over routing entries with a higher metric value. The metric value of the configured routing entries can be specified for the controller.

Besides the manually configurable routes, default gateways can also be set via DHCP replies. A unique metric is assigned to all default gateways assigned by DHCP.

The metric is assigned starting at 10 and depends on the network interface via which the DHCP response was received. The metric is assigned in ascending order based on the alphanumeric sorting of the network interface names (e.g., br0, br1, … wwan0).

Metric example:
A controller obtains its IP configuration via a DHCP server and receives both the

IP address and the network mask 192.168.1.10/24. Furthermore, a gateway with IP address 192.168.1.2 and metric value 20 is set up on the controller. Therefore, when no specific routing entry exists for the target address of network data packets, the controller sends them to gateway 192.168.1.2. Besides the IP address and network mask, the DHCP server is now instructed to allocate a default gateway of 192.168.1.1. The controller gives this default gateway a metric value of 10. Therefore, the default gateway received via DHCP is preferred over the manually configured gateway.

The routing entries are used to specify which gateways the network data packets are sent. If the controller is running in switched mode and only has one network interface, all network traffic passes through this network interface. If the controller is running in separated mode or contains a modem, it has more than one network interface. Therefore, it is possible for a network data packet to arrive at the controller on one network interface and depart on a different network interface. This forwarding between different network interfaces must be explicitly enabled; it is disabled when the controller is delivered. To enable the forwarding, “Enabled” must be enabled in the “IP Forwarding through multiple interfaces” group. In this case, the controller can function as a router.

For forwarding network communication through a router, it is necessary to note that corresponding routing entries must be provided not only for the router, but also for the respective endpoints of the communication. The routing entries of the endpoints must ensure that the desired network data packets are sent via the router, both when the connection is established and with the replies.

Host route example:
A host route is a route to an individual host. In the following example, a route to a host with IP address 192.168.1.2 is to be specified. The route passes through a gateway that can be reached via address 10.0.1.3. To configure a host route to the destination host on a controller connected to the gateway, the following settings must be made:

Destination Address:	192.168.1.2	IP address of the destination host
Destination Mask:	255.255.255.255	Subnet mask of an individual host
Gateway Address:	10.0.1.3	IP address of the gateway
Gateway Metric	20	Route priority

Network route example:
A network route is a route to a subnet, which can contain multiple hosts. In the following example, a route to a subnet should be specified with network address 192.168.1.0. The route passes through a gateway that can be reached via address 10.0.1.3. To configure a network route to the destination network on a controller connected to the gateway, the following settings must be made:

Destination Address:	192.168.1.0	IP address of the destination network
Destination Mask:	255.255.255.0	Subnet mask of the destination network
Gateway Address:	10.0.1.3	IP address of the gateway
Gateway Metric	20	Route priority

Example of a route via an interface:
In the following example, a route to a host with IP address “192.168.1.2” is to be specified. The route runs via the br1 interface, which corresponds to Bridge 2. To configure a host route to the target host via Bridge 2 on a controller with an activated Bridge 2, the following settings must be made.

Destination address:	192.168.1.2	IP address of the target host
Destination mask:	255.255.255.255	Subnet mask of an individual host
Gateway Metric	20	Route priority
Interface	br1	Interface through which the packet is to be routed

Besides configuration of static routes, the controller also supports IP masquerading. This can be enabled for selected network interfaces of the controller. Network data packets that depart the controller through a network interface for which IP masquerading has been enabled are given the IP address of the network interface as their sender address. If network data packets are forwarded through the controller, the network behind the controller is encapsulated under a single address.

Furthermore, the controller permits configuration of port forwarding entries. For port forwarding, the destination address and, if relevant, destination port of a network data packet that arrived at the controller via a previously configured network interface are overwritten. This makes it possible to forward network data packets through the controller to other addresses and ports. Forwarding can be configured for the TCP or UDP protocols.

5.1.4 Network Services

5.1.4.1 DHCP-Client

The controller can get network parameters from an external DHCP master via the DHCP Client service.

The following parameters can be obtained:

- IP address
- SubNet mask
- Router/gateway
- Hostname
- Domain
- DNS server
- NTP server

For the IP address, SubNet mask and router/gateway parameters, the entries are stored per ETHERNET port.

For multiple network interfaces with DHCP, the hostname is taken from the network interface (bridge or Wwan) with the highest priority. The priority is specified alphanumerically by the name of the network interface. Thus, Bridge1 has the highest priority, followed by Bridge2, Bridge3, ..., Wwan0.

5.1.4.2 DHCP Server

The controller provides the DHCP server service for the automatic configuration of IP addresses of network stations on the same subnet.
Generally, only one DHCP server can be active on a subnet at one time.

The following can be set for the DHCP server:

- The service itself (active/not active)
- The range of dynamically assigned IP addresses
- The lease time of the dynamically assigned IP addresses
- A list with static assignments of IP addresses to MAC addresses

In “switched” mode, these settings are possible for both interfaces together and in “separated” mode for each interface separately.

The settings are made, for example, in the WBM via the “DHCP Configuration” page.

The DHCP server also passes other parameters in addition to the IP address. The following table shows the complete list.

Table 25: List of Parameters Transmitted via DHCP

Parameters	Explanation
IP address	An IP address from the range of permitted address; the range can be configured in the WBM. The DHCP server determines the IP address to be passed to the requesting network subscriber (client) from the MAC address of the network subscriber and the range of addresses to be assigned. As long as the configured address range does not change and no bottlenecks occur when assigning IP addresses, the DHCP server continuously reassigns the same IP addresses to requesting network subscribers. When a subscriber connects to the network, for whose MAC address a fixed IP address has been configured in the WBM, this address is passed to it. Such a fixed IP address can also be outside the range of freely-assignable IP addresses. A hostname can also be specified instead of the MAC address for identifying the requesting network subscriber.
Subnet mask	The subnet mask configured in the network settings of the DHCP server for the local network concerned is passed. The subnet mask and IP address determine the range of valid IP addresses on the local network.
Broadcast address	IP address with which an IP packet can be sent to all network subscribers on the subnet at the same time
Lease time	Determines the validity period of the DHCP parameters passed to a network subscriber: Per protocol, the network subscriber is required to request the network settings again after half the period of validity. The lease time is configured in the WBM.
Host name	The network name is passed to the network subscriber. The network subscriber normally sends its own name with its request for the IP address. It is then used by the DHCP server in its response.
Name server	The DHCP server passes its own IP address as the DNS name server to the network subscriber.
Default gateway	The DHCP server passes its own IP address as the default gateway to the network subscriber. The default gateway is required to communication with subscribers outside the local network.

Not all parameters can be set in the WBM. If you want to set other values for the existing parameters or want to pass other parameters via DHCP, the DHCP server must be manually configured. For the controller, the DHCP server service is handled by the program "dnsmasq".

From a Linux® command line, an editor must be used to change the file “/etc/dnsmasq.d/dnsmasq_default.conf” to set the configuration.

5.1.4.3 DNS Server

The controller offers the DNS server service for the automatic assignment of hostnames to IP addresses of network stations.
The DNS server takes over the names and IP addresses of local network stations from the DHCP server. This DNS server routes requests for non-local names, such as from the Internet, to higher-level DNS servers if configured and accessible.

The following settings are possible for the DNS server:

- The service itself (enabled/disabled)
- Access type to the assignments
  The requests are buffered in “Proxy” mode (throughput optimized).
  In Relay mode the requests are routed directly to higher-level name servers.
- A list with up to 15 static assignments of IP addresses to hostnames
  If only the hostname is used, the configured or default domain is added to the hostname automatically to ensure FQDN name resolution.

The settings are made, e.g., in the WBM, via the “Configuration of DNS Service” page.

5.1.5 Cloud Connectivity Functionality

With the cloud connectivity functionality and an IEC library, the controller is available as a gateway for Internet-of-Things (IoT) applications. This means the controller can collect the data from all the connected devices, access the Internet via the built-in Ethernet interface or the mobile communications module and send the data to the cloud.

You can specify the cloud service to use: Microsoft Azure, Amazon Web Services and IBM Cloud are available.

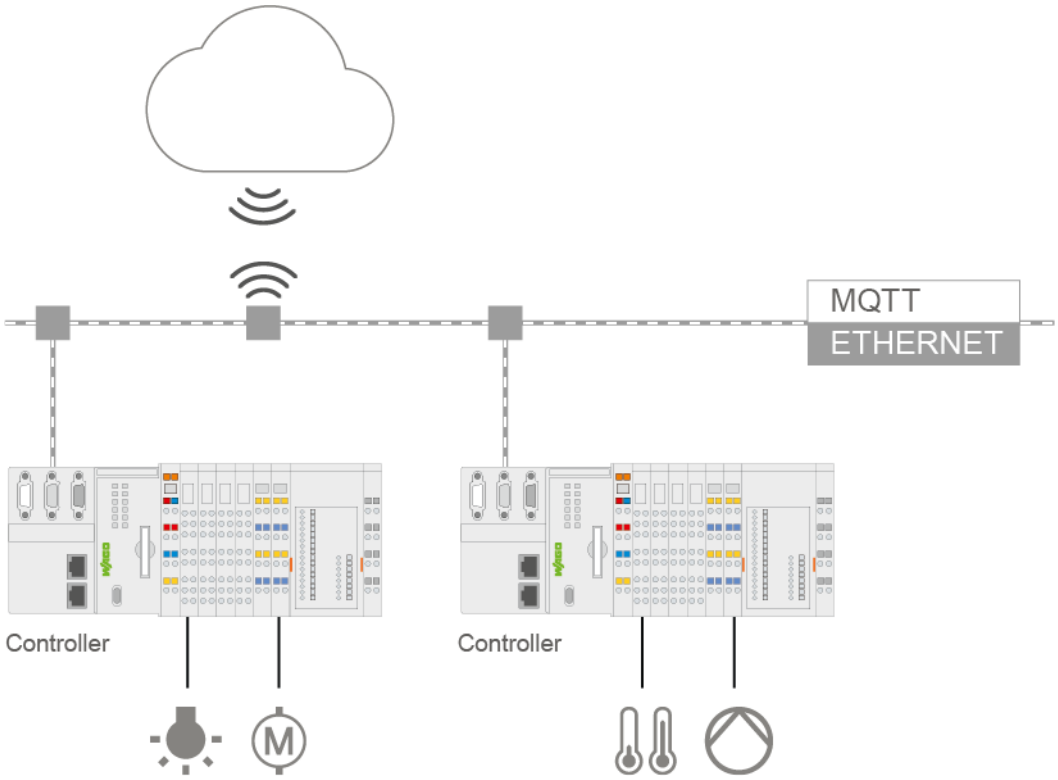


Figure 16: Connecting the Controller to a Cloud Service (Example)

Data is transmitted from the controller to the cloud service as JSON files. The connection can be encrypted with TLS; see the section “Functional Description” > … > “TLS Encryption.”

You can find the settings that must be configured in the controller in order to use the cloud connectivity functionality in the section “Start-Up” > … > “Configuration Using Web-Based Management.

The communication parameter is configured in the WBM; the data to exchange between the cloud and controller is configured with the libraries for ***e!****COCKPIT*.

Note

Please note the risks of using cloud services!
If you use third-party cloud services, sensitive data is transferred to the cloud service provider at one's own responsibility. External access may result in manipulated data and/or unwanted control commands affecting the performance of your control system.

Use encryption methods to protect your data and observe the information provided by the Federal Office for Information Security – “Cloud: Risks and Security Tips”.
Observe comparable publications of the competent, public institutions of your country.

Information

Observe the additional documentation!
You can find a detailed description of the cloud connectivity software package with a controller and information on PLC programming in Application Note A500920 in the Downloads area: www.wago.com.

Information

Observe the necessary data protection and security settings!
Before using the cloud connectivity functionality, consult the corresponding handbook and familiarize yourself with data protection and security issues.
You will find this in the Downloads area at www.wago.com.

5.1.5.1 Components of the Cloud Connectivity Software Package

Table 26: Components of the Cloud Connectivity Software Package

Components	Description
e!*COCKPIT*: WagoAppCloud	IEC library to create the PLC application; function blocks make it possible to exchange data between the PLC and cloud service. The data transmission variables are definable.

5.2 Memory Card Function

Note

Only use recommended memory cards!
Use only the microSD memory card available from WAGO (item No. 758-879/000-3102) as it is suitable for industrial applications subjected to environmental extremes and for use in this device.
Compatibility with other commercially available storage media cannot be guaranteed.

The memory card is optional and serves as an additional memory area in addition to the internal memory or drive in the controller. The user program, user data, source code of the project or device settings can be saved to the memory card, and thus already existing project data and programs can be copied to one or more controllers.

If the memory card is inserted, this is incorporated under /media/sd in the directory structure of the file system inside the controller. This means that the memory card can be addressed like a removable medium on a PC.

The function of the memory card in normal operation and possible faults that may occur when the memory card is used are described in the following sections for different operating modes.

5.2.1 Formatting

Note

Note the pre-formatting of the memory card!
Please note that memory cards ≤ 2 GB are often formatted with the “FAT16” file system type and can generate up to 512 entries in the root directory. For over 512 entries create these in a subdirectory or format the memory card with “FAT32” or “NTFS.”

Note

Memory card access from CODESYS only possible with FAT16, FAT32 or NTFS!
If the CODESYS user “admin” (see the section “Network” > “Network Security” > “Users and Passwords” > “Services and Users“) is supposed to be able to access files created on the memory card, the memory card must be formatted with FAT16, FAT32 or NTFS.
If the Linux® file system formats EXT2 or EXT3 are used, “root” rights are required for data access. Therefore, access via CODESYS is not possible.

5.2.2 Data Backup

The controller has a backup function and a restore function.

In the WBM, the required settings can be made in the “Configuration” tab on the “Package Server” > “Firmware Backup” or “Firmware Restore” pages and the functions can be executed.

Settings can also be made in the CBM menu “Package Server” > “Firmware Backup” or “Firmware Restore”.

The storage medium (internal memory or SD card) and, if applicable, the storage location on the network can be set.

The data to be backed up and restored can also be selected:

- the CODESYS project (“PLC Runtime project,” boot project)
- the device settings (“Settings”)
- the controller operating system and the root file system (“System”)
- all of the above (“All,” only visible if not saved on the network)

Note

Note the firmware version!
Restoring the controller operating system (“System” selection) is only permissible and possible if the firmware versions at the backup and restore times are identical.
If necessary, skip restoring the controller operating system, or match the firmware version of the controller to the firmware version of the backup time beforehand.

5.2.2.1 Backup Function

The backup function enables the data of the internal memory and device settings to be saved on the memory card during operation.

The backup function can be called up the WBM page “Firmware Backup” in the “Configuration” tab, selection “Package Server” > “Firmware Backup” or in the CBM menu “Package Server” > “Firmware Backup”.

The network or the inserted memory card can be selected as the target medium.

The files of the internal drive are stored on the target medium in the directory media/sd/copy and in the corresponding subdirectories.
The information that is not present as files on the controller is stored in XML format in the directory media/sd/settings/.

If the memory card is selected as the target medium, the LED above the memory card slot flashes yellow during the save operation.

The device settings and files of the internal drive are then saved on the target medium.

The controller has an automatic update function. If this function is activated on a memory card before the data backup and a controller is booted from this memory card, this data is restored automatically on the internal memory of the controller.



Note

Only one package may be copied to the network!
If you have specified “Network” as the storage location, only one package may be selected for each storing process.



Note

No backup of the memory card!
Backup from the memory card to the internal flash memory is not possible.



Note

Account for backup time
Generation of backup files can take several minutes. Stop the CODESYS program before you start the backup procedure to help shorten the time required.

5.2.2.2 Restore Function

The restore function is used to load the data and device settings from the memory card to the internal memory during operation.

The restore function can be called up the WBM page “Firmware Restore” in the “Configuration” tab, selection “Package Server” > “Firmware Restore” or in the CBM menu “Package Server” > “Firmware Restore”.

The network or, if it is inserted, the memory card can be selected as the source medium.

If the memory card is selected as the source medium, the LED above the memory card slot flashes yellow during the load operation.

When loading the data, the files are copied from the directory media/sd/copy/ of the source medium to the appropriate directories on the internal memory.

The device has an active and an inactive root partition. The system backup is stored on the inactive partition. Startup is then performed from the newly written partition. If the startup process can be completed, the new partition is switched to active. Otherwise, booting is performed again from the old active partition during the next boot process.

The boot project is loaded automatically and the settings automatically activated after a restart. The “Home directory on memory card enabled” setting determines whether the boot project of the internal drive or the memory card is loaded. This setting can be called up on the WBM page “PLC Runtime Configuration” in the “Configuration” tab, selection “PLC Runtime”.



Note

File size must not exceed the size of the internal drive!
Note that the amount of data in the media/sd/copy/ directory must not exceed the total size of the internal drive.



Note

Restoration only possible from internal memory!
If the device was booted from the memory card, the firmware cannot be restored.



Note

Reset by restore
A reset is performed when the system or settings are restored by CODESYS!



Note

Connection loss through restore
If the restore changes the parameters of the ETHERNET connection, the WBM may then no longer be able to open a connection to the device. You must call the WBM again by entering the correct IP address of the device in the address line.



Note

Note the restore time!
The restore process takes approx. 2 … 3 minutes.
After the restore process, the controller is restarted and is then ready for use again.

5.2.3 Inserting a Memory Card during Operation

The fieldbus nodes and the PLC program are running.

Insert a memory card during ongoing operation.

During normal operation, the memory card is incorporated into the file system of the controller as a drive.
No automatic copy procedures are triggered.

The LED above the memory card flashes yellow during the access.

The memory card is then ready for operation and available under /media/sd.

5.2.4 Removing the Memory Card during Operation

The fieldbus node and the PLC program are in operation and the memory card is plugged in.

Remove the memory card during ongoing operation.



Note

Data can be lost during writing!
Note that if you pull the memory card out during a write procedure, data will be lost.

The LED above the memory card flashes yellow during the attempted access.

The controller then works without a memory card.

5.2.5 Setting the Home Directory for the Runtime System

The home directory for the runtime system is located in the controller's internal memory by default. An existing boot project may be saved in the home directory.

You can use the WBM to move the home directory for the runtime system to the memory card, e.g., to make more memory available for a large boot project or other files.

This setting can be activated using the check box “Home directory on memory card enabled” on the WBM page “PLC Runtime”. Click the **[Submit]** button to apply the setting, which takes effect after the next restart.
No files are applied from the old to the new home directory.

After moving the directory, a project must be loaded and a boot project created.

It should be noted that the memory card may not be removed under any circumstances as long as the home directory is there. If an application is running, system safety can be endangered by an uncontrolled controller crash.

Switching the home directory has no effect if the controller was botted from a memory card. The configuration state is saved, but only takes effect if the content of the memory card is copied to the internal memory.

5.2.6 Load Boot Project

If a boot project exists, it may be loaded, depending on the home directory setting for the runtime system. The following table shows the possible results:

Table 27: Loading a Boot Project

Boot Project Stored in Internal Flash Memory	Memory Card with Boot Project Inserted	"Home Directory on Memory Card Enabled" Checked	Boot Project is Loaded ...
No	No	No	No, no boot project exists
		Yes	No, no boot project exists
	Yes	No	No, no boot project exists in the internal flash memory
		Yes	Yes, from memory card
Yes	no	No	Yes, from internal flash memory
		(Yes) invalid	No, invalid combination, since no boot project is allowed to exist in the internal flash memory for this setting
	Yes	No	Yes, from internal flash memory
		(Yes) invalid	No, invalid combination, since no boot project is allowed to exist in the internal flash memory for this setting

6 Mounting

6.1 Installation Position

Along with horizontal and vertical installation, all other installation positions are allowed.

Note

Use an end stop in the case of vertical mounting!
In the case of vertical assembly, an end stop has to be mounted as an additional safeguard against slipping.
WAGO order no. 249-116 End stop for DIN 35 rail, 6 mm wide
WAGO order no. 249-117 End stop for DIN 35 rail, 10 mm wide

6.2 Overall Configuration

The maximum total length of a fieldbus node without fieldbus coupler/controller is 780 mm including end module. The width of the end module is 12 mm. When assembled, the I/O modules have a maximum length of 768 mm.

Examples:

- 64 I/O modules with a 12 mm width can be connected to a fieldbus coupler/controller.
- 32 I/O modules with a 24 mm width can be connected to a fieldbus coupler/controller.

Exception:

The number of connected I/O modules also depends on the type of fieldbus coupler/controller is used. For example, the maximum number of stackable I/O modules on one PROFIBUS DP/V1 fieldbus coupler/controller is 63 with no passive I/O modules and end module.

NOTICE

Observe maximum total length of a fieldbus node!
The maximum total length of a fieldbus node without fieldbus coupler/controller and without using a 750-628 I/O Module (coupler module for internal data bus extension) may not exceed 780 mm.
Also note the limitations of individual fieldbus couplers/controllers.



Note

Increase the total length using a coupler module for internal data bus extension!

You can increase the total length of a fieldbus node by using a 750-628 I/O Module (coupler module for internal data bus extension). For such a configuration, attach a 750-627 I/O Module (end module for internal data bus extension) after the last I/O module of a module assembly. Use an RJ-45 patch cable to connect the I/O module to the coupler module for internal data bus extension of another module block.

This allows you to segment a fieldbus node into a maximum of 11 blocks with maximum of 10 I/O modules for internal data bus extension.

The maximum cable length between two blocks is five meters.

More information is available in the manuals for the 750-627 and 750-628 I/O Modules.

6.3 Mounting onto Carrier Rail

6.3.1 Carrier Rail Properties

All system components can be snapped directly onto a carrier rail in accordance with the European standard EN 60175 (DIN 35).

NOTICE

Do not use any third-party carrier rails without approval by WAGO!
WAGO Kontakttechnik GmbH & Co. KG supplies standardized carrier rails that are optimal for use with the I/O system. If other carrier rails are used, then a technical inspection and approval of the rail by WAGO Kontakttechnik GmbH & Co. KG should take place.

Carrier rails have different mechanical and electrical properties. For the optimal system setup on a carrier rail, certain guidelines must be observed:

- The material must be non-corrosive.
- Most components have a contact to the carrier rail to ground electro-magnetic disturbances. In order to avoid corrosion, this tin-plated carrier rail contact must not form a galvanic cell with the material of the carrier rail which generates a differential voltage above 0.5 V (saline solution of 0.3 % at 20°C).
- The carrier rail must optimally support the EMC measures integrated into the system and the shielding of the I/O module connections.
- A sufficiently stable carrier rail should be selected and, if necessary, several mounting points (every 20 cm) should be used in order to prevent bending and twisting (torsion).
- The geometry of the carrier rail must not be altered in order to secure the safe hold of the components. In particular, when shortening or mounting the carrier rail, it must not be crushed or bent.
- The base of the I/O components extends into the profile of the carrier rail. For carrier rails with a height of 7.5 mm, mounting points are to be riveted under the node in the carrier rail (slotted head captive screws or blind rivets).
- The metal springs on the bottom of the housing must have low-impedance contact with the DIN rail (wide contact surface is possible).

6.3.2 WAGO DIN Rails

WAGO carrier rails meet the electrical and mechanical requirements shown in the table below.

Table 28: WAGO DIN Rails

Item No.	Description
210-112	35 × 7.5; 1 mm; steel; bluish, tinned, chromed; slotted
210-113	35 × 7.5; 1 mm; steel; bluish, tinned, chromed; unslotted
210-197	35 × 15; 1.5 mm; steel; bluish, tinned, chromed; slotted
210-114	35 × 15; 1.5 mm; steel; bluish, tinned, chromed; unslotted
210-118	35 × 15; 2.3 mm; steel; bluish, tinned, chromed; unslotted
210-198	35 × 15; 2.3 mm; copper; unslotted
210-196	35 × 8.2; 1.6 mm; aluminum; unslotted

NOTICE

Observe the mounting distance of the DIN rail when the load is increased!
With increased vibration and shock load, mount the DIN rail at a mounting distance of max. 60 mm.

6.4 Spacing

The spacing between adjacent components, cable conduits, casing and frame sides must be maintained for the complete fieldbus node.

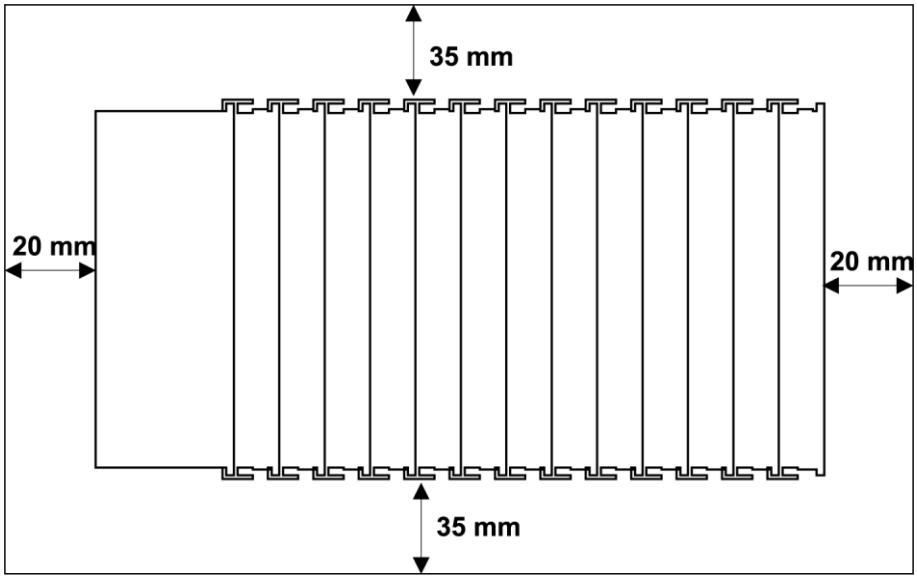


Figure 17: Spacing

The spacing creates room for heat transfer, installation or wiring. The spacing to cable conduits also prevents conducted electromagnetic interferences from influencing the operation.

6.5 Mounting Sequence

Fieldbus couplers, controllers and I/O modules of the WAGO I/O System 750 are snapped directly on a carrier rail in accordance with the European standard EN 60175 (DIN 35).

The reliable positioning and connection is made using a tongue and groove system. Due to the automatic locking, the individual devices are securely seated on the rail after installation.

Starting with the fieldbus coupler or controller, the I/O modules are mounted adjacent to each other according to the project design. Errors in the design of the node in terms of the potential groups (connection via the power contacts) are recognized, as the I/O modules with power contacts (blade contacts) cannot be linked to I/O modules with fewer power contacts.

⚠ CAUTION

Risk of injury due to sharp-edged blade contacts!
The blade contacts are sharp-edged. Handle the I/O module carefully to prevent injury. Do not touch the blade contacts.

NOTICE

Insert I/O modules only from the proper direction!
All I/O modules feature grooves for power jumper contacts on the right side. For some I/O modules, the grooves are closed on the top. Therefore, I/O modules featuring a power jumper contact on the left side cannot be snapped from the top. This mechanical coding helps to avoid configuration errors, which may destroy the I/O modules. Therefore, insert I/O modules only from the right and from the top.



Note

Don't forget the bus end module!
Always plug a bus end module (e.g. 750-600) onto the end of the fieldbus node! You must always use a bus end module at all fieldbus nodes with WAGO I/O System 750 fieldbus couplers or controllers to guarantee proper data transfer.

6.6 Inserting Devices

DANGER

Do not work when devices are energized!
High voltage can cause electric shock or burns.
Switch off all power to the device prior to performing any installation, repair or maintenance work.

6.6.1 Inserting the Controller

1. When replacing the controller for an already available controller, position the new controller so that the tongue and groove joints to the subsequent I/O module are engaged.

2. Snap the controller onto the carrier rail.

3. Use a screwdriver blade to turn the locking disc until the nose of the locking disc engages behind the carrier rail (see the following figure). This prevents the controller from canting on the carrier rail.

With the controller snapped in place, the electrical connections for the data contacts and power contacts (if any) to the possible subsequent I/O module are established.

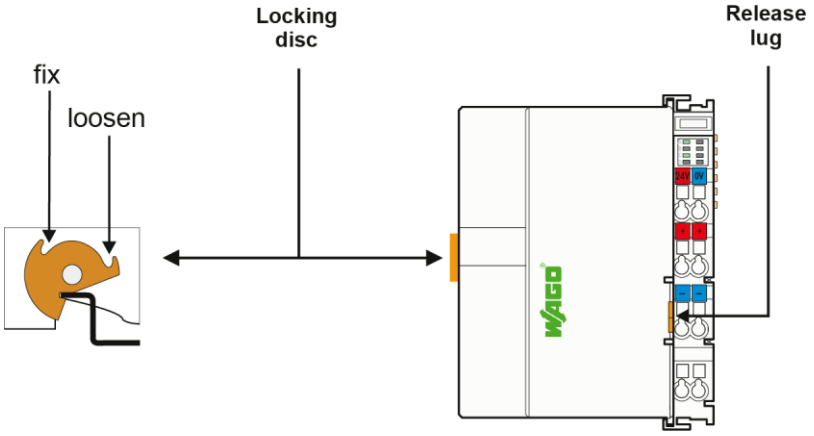


Figure 18: Release Tab of Controller (Example)

7 Connect Devices

7.1 Connecting a Conductor to the CAGE CLAMP®

The WAGO CAGE CLAMP® connection is appropriate for solid, stranded and finely stranded conductors.

NOTICE

Select conductor cross sections as required for current load!
The current consumed for field-side supply may not exceed 10 A. The wire cross sections must be sufficient for the maximum current load for all of the I/O modules to be supplied with power.

Note

Only connect one conductor to each CAGE CLAMP® connection!
Only one conductor may be connected to each CAGE CLAMP® connection.
Do not connect more than one conductor at one single connection!

If more than one conductor must be routed to one connection, these must be connected in an up-circuit wiring assembly, for example using WAGO feed-through terminals.

1. To open the CAGE CLAMP® insert the actuating tool into the opening above the connection.
2. Insert the conductor into the corresponding connection opening.
3. To close the CAGE CLAMP® simply remove the tool - the conductor is then clamped firmly in place.

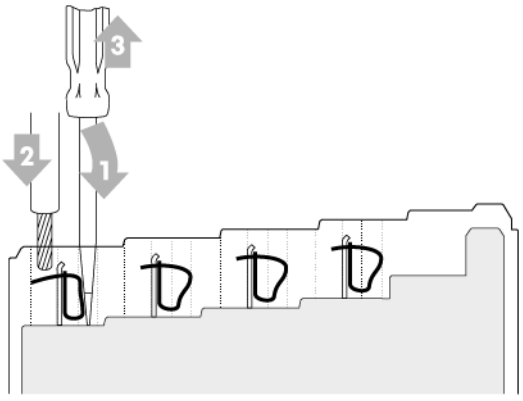


Figure 19: Connecting a Conductor to a CAGE CLAMP®

7.2 Power Supply Concept

7.2.1 Overcurrent Protection

⚠ WARNING

Possible fire hazard due to insufficient overcurrent protection!
In the event of a fault, insufficient overcurrent protection can present a possible fire hazard. In the event of a fault, excessive current flow in the components can cause significant overheating. Therefore, you should always dimension the overcurrent protection according to the anticipated power usage.

The system and field voltage of the WAGO-I/O-SYSTEMs 750 is supplied on the head stations and bus supply modules.
For components that work with extra low voltage, only SELV/PELV voltage sources should be used.

A single voltage source supplying multiple components must be designed according to the component with the strictest electrical safety requirements.
For components which are only allowed to be supplied by SELV voltage sources, these requirements are listed in the technical data.

Most components in the WAGO-I/O-SYSTEM 750 have no internal overcurrent protection. Therefore, appropriate overcurrent production must always be implemented externally for the power supply to these components, e.g. via fuses.
The maximum permissible current is listed in the technical data of the components used.

NOTICE

System supply only with appropriate fuse protection!
Without overcurrent protection, the electronics can be damaged.
If you implement the overcurrent protection for the system supply with a fuse, a fuse, max. 2 A, slow-acting, should be used.

NOTICE

Field supply only with appropriate fuse protection!
Without overcurrent protection, the electronics can be damaged.
If you alternatively implement the overcurrent protection for the field supply with an external fuse, a 10 A fuse should be used.

7.2.2 Supplementary Power Supply Regulations

The WAGO-I/O-SYSTEM 750 can also be used in shipbuilding or offshore and onshore areas of work (e. g. working platforms, loading plants). This is demonstrated by complying with the standards of influential classification companies such as Germanischer Lloyd and Lloyds Register.

Filter modules for 24 V supply are required for the certified operation of the system.

Table 29: Filter Modules for 24 V Supply

Order No.	Name	Description
750-626	Supply Filter	Filter module for system supply and field supply (24 V, 0 V), i. e. for fieldbus coupler/controller and bus power supply (750-613)
750-624	Supply Filter	Filter module for the 24 V field supply (750-602, 750-601, 750-610)

Therefore, the following power supply concept must be absolutely complied with.

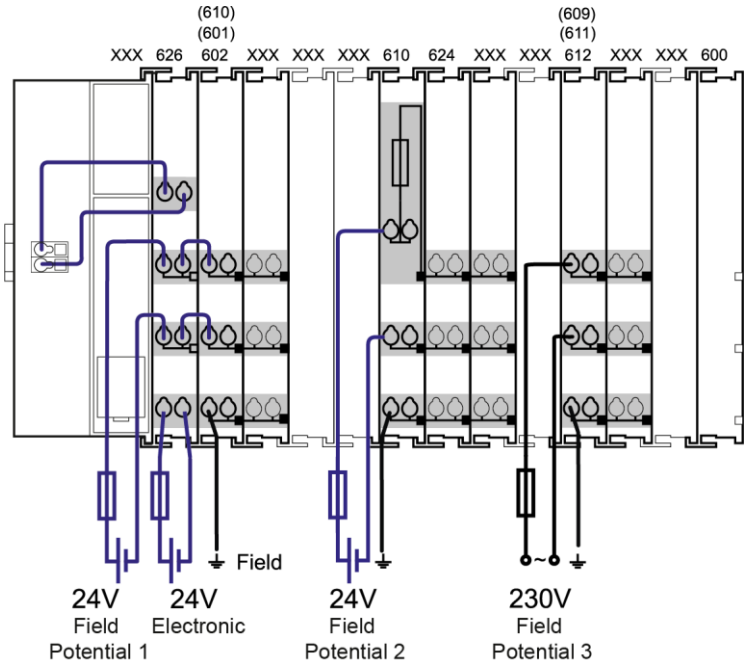


Figure 20: Power Supply Concept

Note

Use a supply module for equipotential bonding!
Use an additional 750-601/ 602/ 610 Supply Module behind the 750-626 Filter Module if you want to use the lower power jumper contact for equipotential bonding, e.g., between shielded connections and require an additional tap for this potential.

8 Commissioning

Note

Close any ports and services that you do not need!
Unauthorized persons may gain access to your automation system through open ports.
To reduce the risk of cyber attacks and, thus, enhance your cyber security, close all ports and services in the control components (in particular Port 6626 for WAGO I/O-*CHECK*, Port 2455 for CODESYS 2 and Port 11740 for ***e!****COCKPIT*) not required by your application.
Only open ports and services during commissioning and/or configuration.

8.1 Switching On the Controller

Before switching on the controller ensure that you

- have properly installed the controller (see section “Installation”),
- have connected all required data cables (see section “Connections”) to the corresponding interfaces and have secured the connectors by their attached locking screws,
- have connected the electronics and field-side power supply (see section “Connections”),
- have mounted the end module (see Section “Installation”),
- have performed appropriate potential equalization at your machine/system (see System Description for 750-xxx) and
- have performed shielding properly (see System Description for 750-xxx).

To switch on both the controller and the connected I/O modules, switch on your power supply unit.

Starting of the controller is indicated by a brief orange flashing of all LEDs. After a few seconds the SYS LED will indicate successful boot-up of the controller.
The runtime system ***e!****RUNTIME* is started at the same time.

Once the entire system has been successfully started, the SYS and I/O LEDs light up green.

If there is an executable IEC 61131-3 program stored and running on the controller, the RUN LED will light up green.

If no executable program is stored on the controller, or the mode selector switch is set to STOP, this is likewise indicated by the RUN LED (see Section “Diagnostics”> … > “Fieldbus/System Indication Elements”).

8.2 Determining the IP Address of the Host PC

To ensure that the host PC can communicate with the controller via ETHERNET, both devices must be located in the same subnet.

To determine the IP address of the host PC (with the Microsoft Windows® operating system) using the MS DOS prompt, proceed as follows:

1. Open the MS DOS prompt window.
   To do this, enter the command “cmd” in the input field under **Start** > **Execute…** > **Open:** (Windows® XP) or **Start** > **Search programs/files** (Windows® 7) and then click **[OK]** or press **[Enter]**.

2. In the MS DOS prompt enter the command “ipconfig” and then press **[Enter]**.

3. The IP address, subnet mask and standard gateway, including the appropriate parameters, are displayed.

8.3 Setting an IP Address

In the controller's initial state, the following IP addresses are active for the ETHERNET interface (Port X1 and Port X2):

Table 30: Default IP Addresses for ETHERNET Interfaces

ETHERNET Interface	Default Setting
X1/X2 (switched mode)	Dynamic assignment of IP address using DHCP ("Dynamic Host Configuration Protocol")

Adapt IP addressing to your specific system structure to ensure that the PC and the controller can communicate with one another using one of the available configuration tools (see section "Configuration").

Example for incorporating the controller (192.168.2.17) into an existing network:

- The IP address of the host PC is **192.168.1.2**.
- The controller and host PC must be in the same subnet (regardless of the IP address of the host PC).
- With a subnet mast of **255.255.255.0**, the first three digits of the IP address of the host PC and controller must match so that they are located in the same subnet.

Table 31: Network Mask 255.255.255.0

Host PC	Subnet Address Range for the Controller
192.168.1.2	**192.168.1**.1 or **192.168.1**.3 … **192.168.1**.254

8.3.1 Assigning an IP Address using DHCP

The Controller can obtain dynamic IP addresses from a server (DHCP/BootP). In contrast to fixed IP addresses, dynamically assigned addresses are not stored permanently. Therefore, a BootP or DHCP server must be available each time the controller is restarted.

If an IP address has been assigned by means of DHCP (default setting), it can be determined through the settings and the output of the specific DHCP server.

In the example figure shown here, the corresponding output of “Open DHCP” is presented.

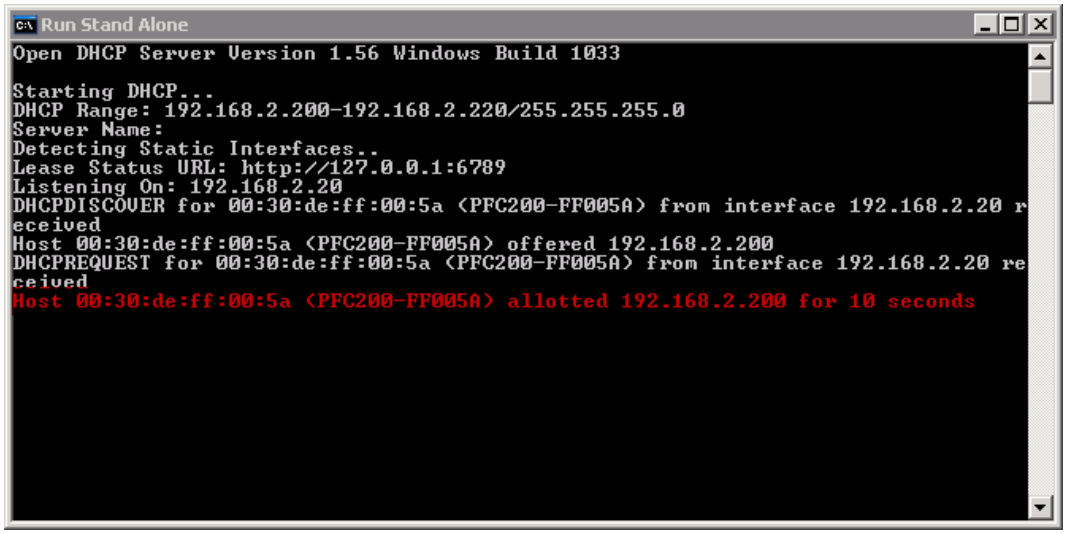


Figure 21: “Open DHCP”, Example Figure

In conjunction with the DNS server associated with DHCP, the device can be reached using its host name.
This name consists of the prefix “PFCx00-“ and the last six places of the MAC address (in the example shown here: “00:30:DE:FF:00:5A”). The MAC address of the device can be printed on the label on the side of the device.

The host name of the device in the example shown here is thus “PFC200-FF005A”.

8.3.2 Changing an IP Address Using the “CBM” Configuration Tool and a Terminal Program

You can also assign a new IP address to the ETHERNET interfaces X1 and X2 using the “CBM” configuration tool provided on the Linux® console. More information about “CBM” is given in the Section “Configuration.”

1. Connect a PC to the ETHERNET interface X1 of the controller using an SSH terminal program.

2. Start the terminal program.

3. Select “SSH” as the connection type, and enter the IP address of the controller and port 22 as the connection parameters.

4. Log in to the Linux® system as a “super user.”
   The user name and the password are provided in the Section “Users and Passwords” > “Linux® User Group.”

5. Start the configuration tool by entering the command “cbm” (case sensitive) on the command line and then press **[Enter]**.

```
================================================================================
 WAGO Console Based Management Tool
================================================================================
 Main Menu
--------------------------------------------------------------------------------
 0. Quit
 1. Information
 2. PLC Runtime
 3. Networking
 4. Firewall
 5. Clock
 6. Administration
 7. Package Server
 8. Mass Storage
 9. Software Uploads
 10. Ports and Services
 11. SNMP
 12. PROFIBUS DP
--------------------------------------------------------------------------------
 Select an entry or Q to quit
--------------------------------------------------------------------------------
```

Figure 22: CBM main menu (example)

6. In the **Main menu** use the keyboard (arrow keys or numeric keypad) to move to and select **Networking** and then press **[Enter]**.

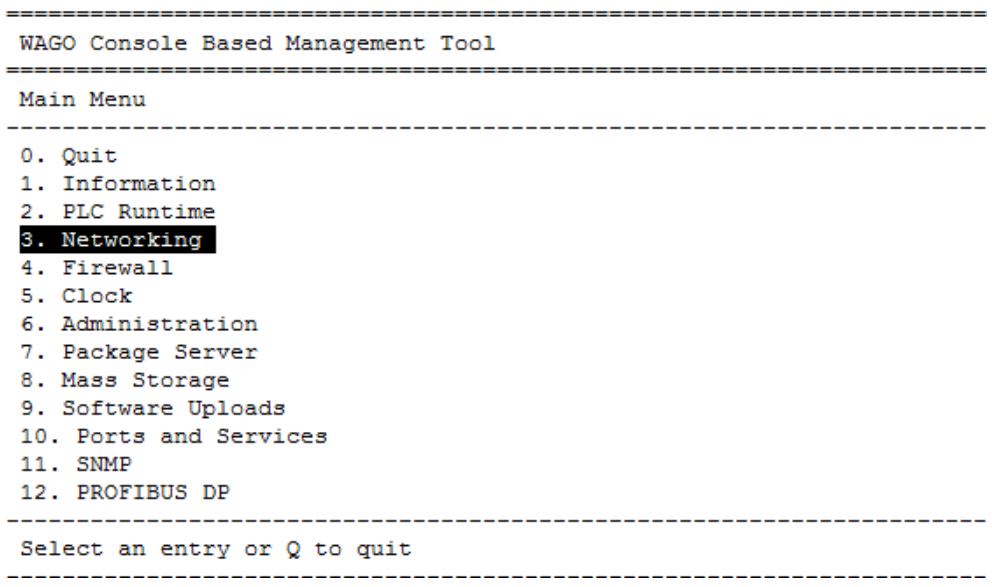


Figure 23: CBM – Selecting “Networking”

7. In the **Networking** menu select **TCP/IP** and press **[Enter]**.

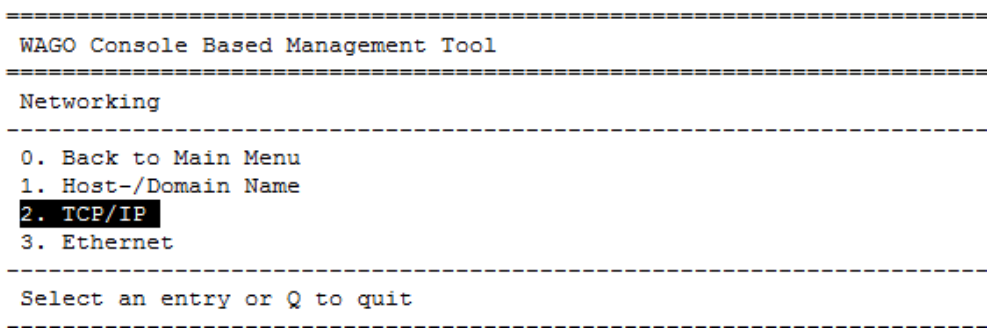


Figure 24: CBM – Selecting “TCP/IP”

8. In the menu **TCP/IP** select **IP Address** and press **[Enter]**.

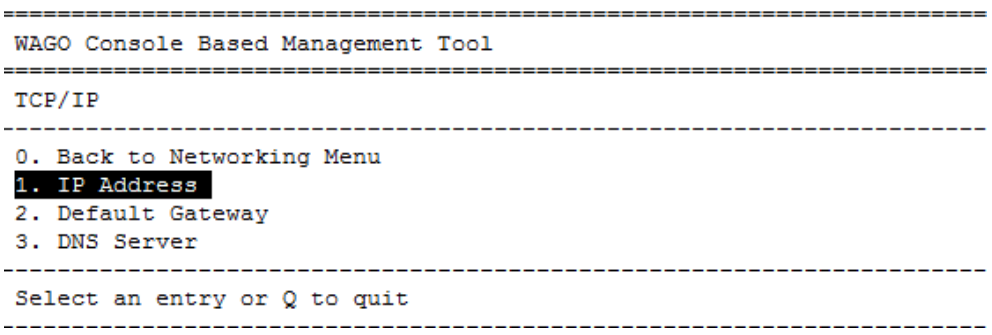


Figure 25: CBM – Selecting “IP address”

9. In the menu **TCP/IP Configuration** select **IP Address** and press **[Enter]**.

```
================================================================================
 WAGO Console Based Management Tool
================================================================================
 TCP/IP Configuration of X1
--------------------------------------------------------------------------------
 0. Back to TCP/IP Menu
 1. Type of IP Address Configuration....Static IP
 2. IP Address.........................192.168.1.18
 3. Subnet Mask........................255.255.255.0
--------------------------------------------------------------------------------
 Select an entry or Q to quit
--------------------------------------------------------------------------------
```

Figure 26: CBM – Selecting the IP Address

10. In the menu **Change IP Address** enter the new IP address and confirm by clicking **[OK]**. If you want to return to the main menu without making changes, click **[Abort]**.

```
================================================================================
 WAGO Console Based Management Tool
================================================================================
 Change IP Address
--------------------------------------------------------------------------------

 Enter new IP Address:
 +---------------+
 |192.168.1.17   |
 +---------------+

 < OK >    <Abort>

--------------------------------------------------------------------------------
 OK: confirm value, Abort: quit without changes
--------------------------------------------------------------------------------
```

Figure 27: CBM – Entering a New IP Address

8.3.3 Changing an IP Address using “WAGO Ethernet Settings”

The Microsoft Windows® application “WAGO Ethernet Settings” is a software used to identify the controller and configure network settings.

Note

Observe the software version!

To configure the controller use at least Version 6.4.1.1 dated 2015-06-29 of “WAGO Ethernet Settings”!

You can use WAGO communication cables or WAGO radio adapters or even the IP network for data communication.

1. Switch off the power supply to the controller.
2. Connect the 750-920 communication cable to the Service interface on the controller and to a serial interface of your PC.
3. Switch the power supply to the controller on again.
4. Start the “WAGO Ethernet Settings” program.

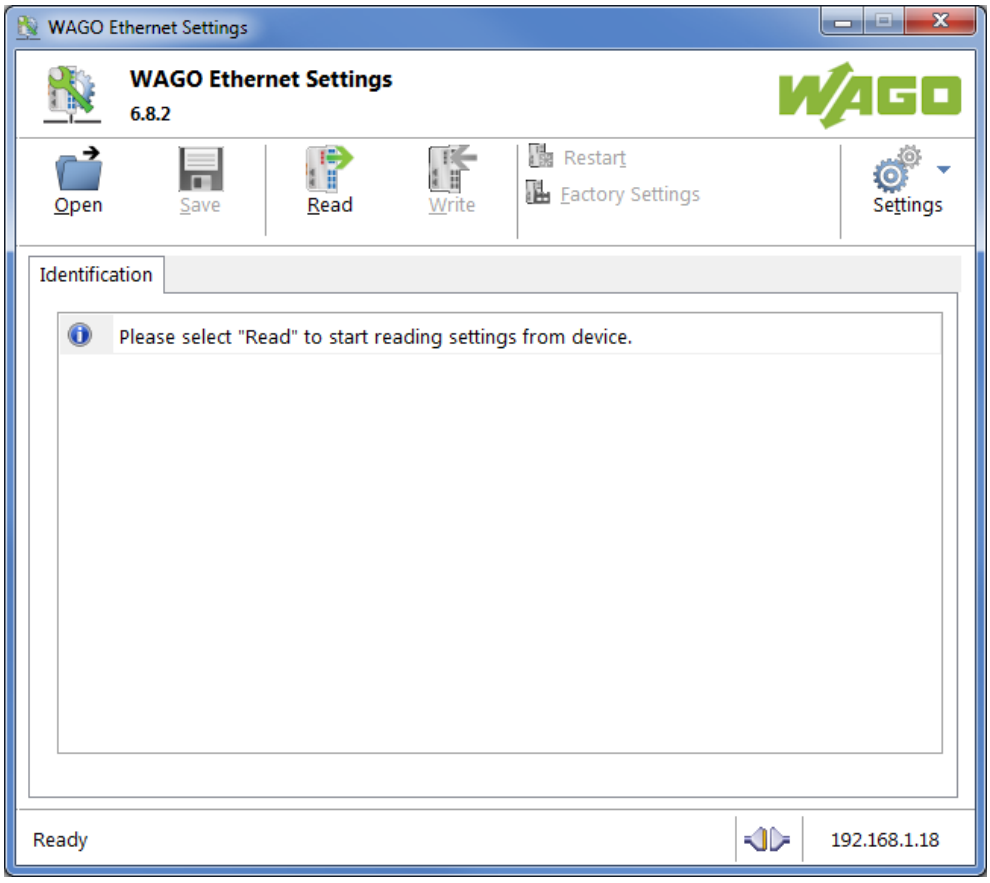


Figure 28: “WAGO Ethernet Settings” – Starting Screen (Example)

5. Click **[Read]** to read in and identify the connected controller.

6. Select the “Network” tab:

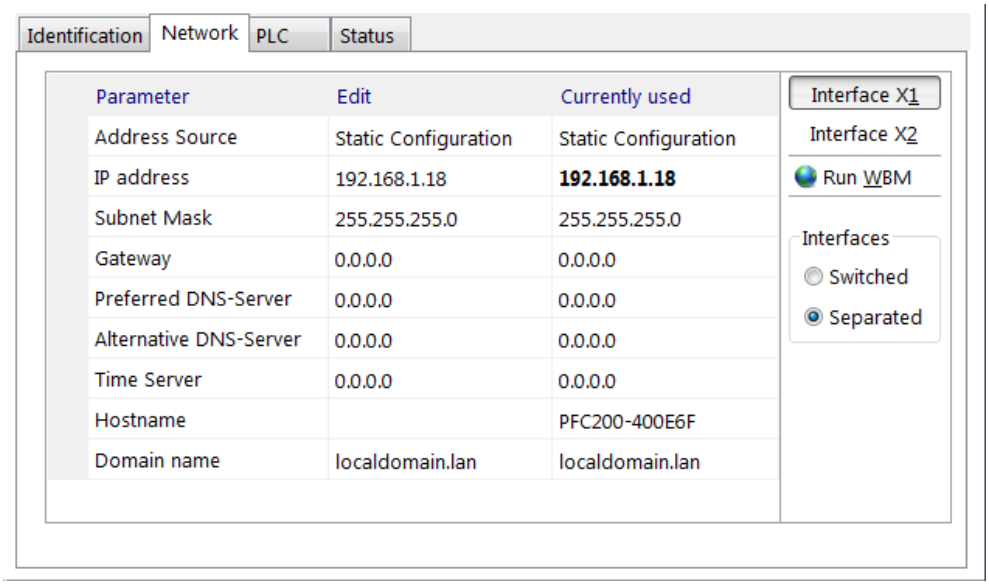


Figure 29: “WAGO Ethernet Settings” – “Network” Tab

7. To assign a fixed address, select “Static configuration” on the “Source” line under “Input”. DHCP is normally activated as the default setting.

8. In the column “Input” enter the required IP address and, if applicable, the address of the subnet mask and of the gateway.

9. Click on **[Write]** to accept the address in the controller. (If necessary, “WAGO Ethernet Settings” will restart your controller. This action may require about 30 seconds.)

10. You can now close “WAGO Ethernet Settings”, or make other changes directly in the Web-based Management system as required. To do this, click on **[Run WBM]** at the right in the window.

8.3.4 Setting the IP Address with the Address Selection Switch

For the “PFC100; 2ETH; ECO” controller (750-8100), you can change the network settings using the address selection switch. The address selection switch is above the X1 and X2 network ports.

The address selection switch includes switches 1 … 8 with the weight 1 … 128. A disabled switch has the value 0. The set address value is derived from the sum of the weight of all enabled switches (example: Switches 7, 6 and 3 to “ON” corresponds to the address value 64 + 32 + 4 = 100). You can set an address value of 0 … 255.

The address selection switch setting only queried when restarting the controller. Changing the switch positions during operation are ignored until the next restart.

If you operate the X1 and X2 ETHERNET interfaces in Separated mode, the settings only apply to the X1 interface. All settings remain unchanged for the X2 interface.
If you operate the X1 and X2 ETHERNET interfaces in Switched mode, the settings apply to both the X1 and X2 interfaces.

The following table shows the significance of the address values of the address selection switch.

Table 32: Significance of the Address Values of the Address Selection Switch

Address value	Explanation
0	The IP parameters are configured via the settings in the Web-Based Management (WBM), Console-Based Management (CBM) or by the factory settings.
1 … 254	A fixed IP address is assigned. The IP address consists of the network address and the set address value. The network address can be configured from the CBM or WBM and is 192.168.1 by default.
255	The DHCP protocol is used to configure the IP parameters.

A fixed IP address consists of a base address and the address value setting from the address values 1 … 254. The IP address for X1 that can be set from the CBM/WBM is used as the base address. The netmask is also taken into account when composing the fixed IP address. The address selection switch always changes the complete device-specific part of the IP address. A program restart is required for the change to the address selection switch to take effect.

Examples:

The IP address setting is 192.168.129.129;
the address selection switch is set to the value 203.

The entire fourth value of the IP address is replaced when the netmask is 255.255.255.0.

Netmask setting:	255.255.255.000
IP address setting:	192.168.129.129
Resulting network address:	192.168.129.000
Resulting device address:	---.---.---.129
Address selection switch:	---.---.---.203
Network address after restart:	192.168.129.000
Device address after restart:	---.---.---.203
IP address after restart:	192.168.129.203

254 address are possible and can be set (1 … 254).

If the netmask is larger (e.g. 255.255.255.240), the address value is limited. Only some of the DIP switches of the address switch are taken into account. In the following example, these are only switches 1 ... 4. The setting of switches 5 ... 8 is ignored.

Netmask setting:	255.255.255.240
IP address setting:	192.168.129.129
Resulting network address:	192.168.129.128
Resulting device address:	---.---.---.001
Address selection switch:	---.---.---.203
Network address after restart:	192.168.129.128
Device address after restart:	---.---.---.011
IP address after restart:	192.168.129.139

254 addresses can be set (1 … 254), but only 14 addresses (1 … 14) are possible.

If the netmask is lower (e.g. 255.255.240.000), the possible number of devices on one subnet increases, but only some of the possible device addresses can be set with the address switch.

Netmask setting:	255.255.240.000
IP address setting:	192.168.129.129
Resulting network address:	192.168.128.000
Resulting device address:	---.---.--1,129
Address selection switch:	---.---.---.203
Network address after restart:	192.168.128.000
Device address after restart:	---.---.---.203
IP address after restart:	192.168.128.203

4094 addresses are possible (1 … 4094), but only 254 addresses can be set (1 … 254).

8.3.5 Temporarily Setting Fixed IP Addresses

This process temporarily sets the IP addresses for the network interfaces X1 … X<n> to fixed IP addresses.
For each bridge used, the assigned interfaces are assigned their own address, whereby bridge 1 receives the IP address “192.168.1.17”, bridge 2 the IP address “192.168.2.17” and so on.

No reset is performed.

To set temporary fixed IP addresses, proceed as follows:

1. Set the mode selector switch to STOP and

2. Press and hold the Reset button (RST) for longer than 8 seconds.

Execution of the setting is signaled by the “SYS” LED flashing orange.

If you make changes to the IP configuration of a bridge after activating the temporary IP addresses, the new settings are permanently adopted and applied immediately. The configured bridge exits the temporary IP address mode. The other bridges keep the temporarily set IP address until restart / reset.

To cancel this setting, proceed as follows:

- Perform a software reset or

- Switch off the controller and then switch it back on.

8.4 Testing the Network Connection

Carry out a ping network function to check whether you can reach the controller at the IP address you have assigned in the network.

1. Open the MS DOS prompt window.
   To do this, enter the command “cmd” in the input field under **Start** > **Execute…** > **Open:** (Windows® XP) or **Start** > **Search programs/files** (Windows® 7) and then click **[OK]** or press **[Enter]**.

2. In the MS DOS window, enter the command “ping” and the IP address of the controller (for example, `ping 192.168.1.17)` and then press **[Enter]**.

Note

Host entries in the ARP table!

It may also be useful to delete the current host entries in the ARP table with the command “arp -d *” before executing the “ping” command (as administrator in Windows® 7). This ensures that older entries will not impair the success of the “ping” command.

3. Your PC sends out a query that is answered by the controller. This reply appears in the MS DOS prompt window. If the error message “Timeout” appears, the controller has not responded properly. You then need to check your network settings.

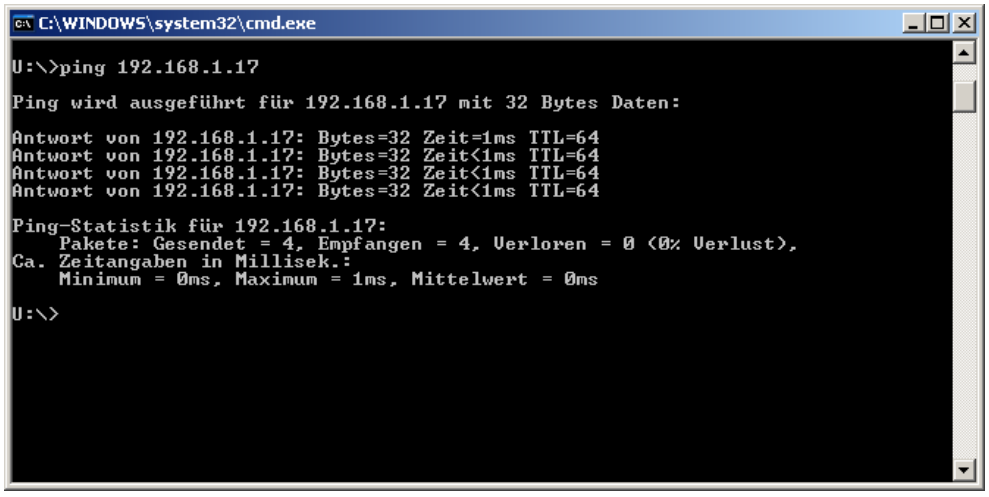


Figure 30: Example of a Function Test

4. If the test is completed successfully, close the MS DOS window.

8.5 Changing Passwords



Note

Change standard passwords
The standard passwords are documented in these instructions and therefore do not offer adequate protection! Change the passwords to meet your particular needs!

To increase security all passwords should contain a combination of lower case letters (a … z), upper case letters (A … Z), numbers (0 … 9), spaces and special characters: (]!"#$%&'()*+,./:;<=>?@[\^_`{|}~-). Passwords should not contain generally known names, dates of birth and other information that is easy to guess.

Change the standard passwords before commissioning the controller.
Standard passwords are issued for the user groups “WBM Users” and “Linux® Users.”

The table in the Section “Function Description” > ... > “Users and Passwords” > “WBM Users Group” shows the standard passwords for the WBM users. Proceed as follows to change these passwords:

1. Connect the controller to a PC via one of the network interfaces (X1, X2).
2. Start a web browser program on the PC and call up the WBM of the controller (see Section “Commissioning” > … > “Configuration via Web-Based-Management (WBM)”).
3. Log in on the controller as “admin” user with the standard password.
4. Change the password for all users on the WBM “Configuration of the users for the WBM” page.
5. Select each user and enter a new password and confirm it.

The table in the Section “Functional Description” > ... > “Users and Passwords” > “Linux® Users Group” shows the standard passwords for the Linux® users. Proceed as follows to change these passwords:

1. Connect the controller to a PC via the network interfaces X1.
2. Start a terminal program on the PC (see Section “Commissioning” > … > “Configuration via Console-Based-Management-Tool (CBM) using a Terminal Program”).
3. Log in on the controller as user “root” with the standard password.
4. Change the password for all users with the “passwd root,” “passwd admin” and “passwd user” commands.

8.6 Shutdown/Restart

Switch off the power supply to shut down the controller.

To perform a controller restart, press the Reset button as described in the Section “Triggering Reset Functions” > “Software Reset (Restart).”
Alternatively, you can switch off the controller and switch it back on again.



Note

Do not power cycle the controller after changing any parameters!
Some parameter changes require a controller restart for the changes to apply. Saving changes takes time.
Do not power cycle the controller to perform a restart, i.e., changes may be lost by shutting down the controller too soon.
Only restart the controller using the software reboot function. This ensures that all memory operations are completed correctly and completely.

8.7 Initiating Reset Functions

You can initiate various reset functions using the mode selector switch and the Reset button (RST).

8.7.1 Warm Start Reset

All ***e!****RUNTIME* applications are reset with a warm start reset. All global data is set to its initialization values. This corresponds to the ***e!****COCKPIT* IDE “Reset warm” command.

To perform a warm start reset, set the mode selector switch to "Reset" and hold it there for two to seven seconds.
Execution of the reset is signaled by the red “RUN LED” briefly going out when the mode selector switch is released.

8.7.2 Cold Start Reset

All ***e!****RUNTIME* applications are reset with a cold start reset. All global data and the retain variables are set to their initialization values.
This corresponds to the ***e!****COCKPIT* IDE “Reset Cold” command.

To perform a cold start reset, set the mode selector switch to “Reset” and hold it there for more than seven seconds.
Execution of the reset is signaled after seven seconds by the “RUN” LED going out for an extended period. You can then release the mode selector switch.

8.7.3 Software Reset

The controller is restarted on a software reset.

To perform a software reset, set the mode selector switch to RUN or STOP and then press the Reset button (RST) for one to eight seconds.

Reset completion is indicated by a brief orange flashing of all LEDs. After a few seconds the SYS LED will indicate successful boot-up of the controller.

8.7.4 Controller Reset

NOTICE

Do not switch the controller off!
The controller can be damaged by interrupting the controller reset process.
Do not switch the controller off during the controller reset process, and do not disconnect the power supply!

Note

Parameters and passwords are overwritten!
Parameters and passwords for the Linux® and WBM users of the controller are overwritten by a controller reset.
Stored boot projects are deleted, including existing web visualizations.
Subsequently installed firmware functions are not overwritten.
Software licenses are retained.
The inactive system is not changed by the reset.
If you have any questions, contact WAGO Support.

The controller is restarted after the controller reset.
Proceed as follows to reset the controller:

1. Press the Reset button (RST).
2. Set the mode selector switch to the “RESET” position.
3. Press and hold both buttons until the “SYS” LED alternately flashes red/green after approx. 8 seconds.
4. When the “SYS” LED flashes red/green alternately, release the mode selector switch and Reset button.

Note

Do not interrupt the reset process!
If you release the Reset button (RST) too early, then the controller restarts without performing the controller reset.

8.8 Configuration



Note

Check firmware version and update if required!
At the beginning of initial configuration check to ensure that you have the latest firmware version for the controller.
The firmware version installed on the controller is given on the WBM page “Status Information”, or in the CBM menu “Information” under “Controller Details”.
Perform an update to install the latest firmware version.
To do this, follow the instructions given in section “Service” > “Firmware Changes” > “Perform Firmware Upgrade”.

The following methods are available for configuring the controller:

- Access to the Web-based management system via the PC using a web browser (section “Configuration Using Web-Based Management [WBM]”)
- Access to the “Console-Based Management” tool via the PC using a terminal program (section “Configuration Using a Terminal Program [CBM]”)
- Access via the PLC program CODESYS using the “WagoAppConfigTool.lib” library.
- Access via the PC using “WAGO Ethernet Settings” (section “Configuration Using ‘WAGO Ethernet Settings’”).

The CBM is basically for the initial configuration and startup of the controller. Therefore, it only provides a subset of the WBM parameters. For example, parameters that cannot be displayed in a terminal window in a reasonable way and are not necessary for initial startup are not displayed. You can find the explanations of the parameters starting with the section “‘Information’ Page.”

8.8.1 Configuration via Web-Based-Management (WBM)

The HTML pages (from here on referred to as “pages”) of the Web-Based Management are used to configure the controller. Proceed as follows to access the WBM using a web browser:

1. Connect the controller to the ETHERNET network via the ETHERNET interface X1.

2. Start a Web browser on your PC.

3. Enter “https://” followed by the controller's IP address and “/wbm-ng” in the address line of your web browser, e.g., “https://192.168.1.17/wbm-ng”.
   Note that the PC and the controller must be located within the same subnet (see Section “Setting an IP Address”).
   If you do not know the IP address and cannot determine it, switch the controller temporarily to the pre-set address “192.168.1.17” (“Fixed IP address” mode, see Section “Commissioning” > … > “Temporarily Setting a Fixed IP Address”).

Note

Take usage by the CODESYS program into account
If the controller is at capacity due to a CODESYS program, this may result in slower processing in the WBM. As a result, timeout errors are sometimes reported in some circumstances. It is therefore important to stop the CODESYS application prior to performing complicated configurations using WBM.

→ When the connection has been established, a login window opens.

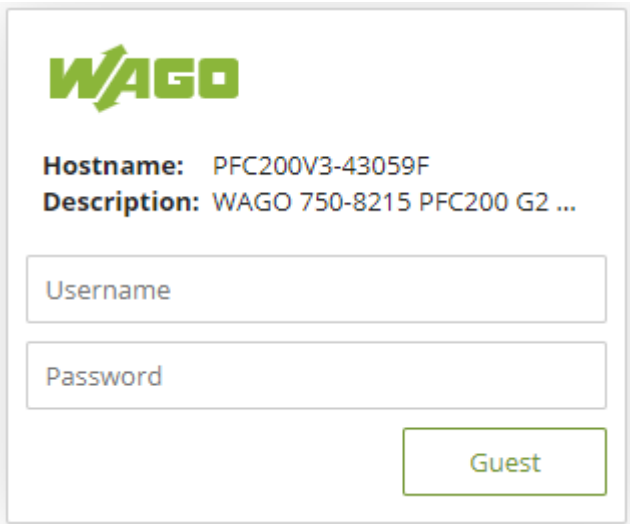


Figure 31: Entering Authentication

4. Enter the username and password.

5. Click the **[Login]** button.

6. If you only want to log in as a guest, click the **[Guest]** button.

→ Depending on the user selected, the navigation bar and the tabs of the WBM are displayed.

If you have disabled cookies in your web browser, you can continue to use the WBM as long as you move directly inside it. However, if you fully reload the website (e.g., with **[F5]**), you must log in again since the web browser is then not able to store the data of your login session.

8.8.1.1 WBM User Administration

To allow settings to be made only by a select number of users, limit access to WBM functions through User Administration.

Note

Change passwords
Default passwords are documented in these instructions and therefore do not offer adequate protection! Change the passwords to meet your particular needs.

If you do not change these passwords, a warning will appear each time you call up a website after logging in.

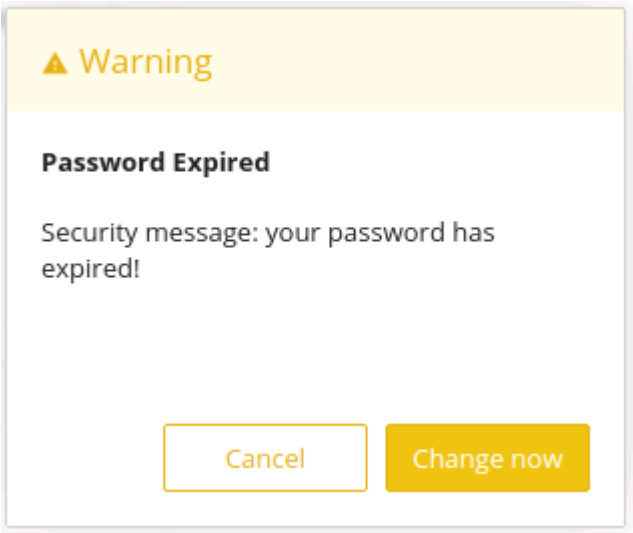


Figure 32: Password Reminder

Table 33:User Settings in the Default State

Users	Permissions	Default Password
root	All (administrator)	wago
admin	All (administrator)	wago
user	Supported to a limited extent	user
guest	Display only	---

Note

General Rights of WBM Users
The WBM users “root”, “admin” and “user” have rights beyond the WBM to configure the system and install software.

User administration for controller applications is configured separately.

Access rights for the WBM pages are shown in the table below.
The “root” user has the same rights as the “admin” user and is therefore not listed separately.

Table 34: Access Rights for WBM Pages

Tab/Navigation	WBM Page Title	User
Information		
Device Status	Device Status	guest
Vendor Information	Vendor Information	guest
PLC Runtime	PLC Runtime Information	guest
Legal Information		
WAGO Licenses	WAGO Software License Agreement	guest
Open Source Licenses	Open Source Licenses	user
WBM Licenses	WBM Third Party License Information	user
Trademarks Information	Trademarks Information	guest
WBM Version	WBM Version Info	guest
Configuration		
PLC Runtime	PLC Runtime Configuration	user
Networking		
TCP/IP Configuration	TCP/IP Configuration	user
Ethernet Configuration	Ethernet Configuration	user
Host/Domain Name	Configuration of Host and Domain Name	user
Routing	Routing	user
Clock	Clock Settings	user
Administration		
Service Interface	Configuration of Service Interface	admin
Create Image	Create bootable Image	admin
Package Server		
Firmware Backup	Firmware Backup	admin
Firmware Restore	Firmware Restore	admin
Active System	Active System	admin
Mass Storage	Mass Storage	admin
Software Uploads	Software Uploads	admin
Ports and Services		
Network Services	Configuration of Network Services	admin
NTP Client	Configuration of NTP Client	admin
PLC Runtime Services	PLC Runtime Services	admin
SSH	SSH Server Settings	admin
TFTP	TFTP Server	admin
DHCP Server	DHCP Server Configuration	admin

Table 34: Access Rights for WBM Pages

Tab/Navigation			WBM Page Title	User
		DNS	Configuration of DNS Service	user
	Cloud Connectivity			
		Status	Overview	admin
		Connection 1	Configuration	admin
		Connection 2	Configuration	admin
	SNMP			
		General Configuration	Configuration of general SNMP parameters	admin
		SNMP v1/v2c	Configuration of SNMP v1/v2c parameters	admin
		SNMP v3	Configuration of SNMP v3 Users	admin
	Users		WBM User Configuration	admin
Fieldbus				
	OPC UA			
		Status	OPC UA Status	admin
		Configuration	OPC UA Configuration	admin
		Server Certificates	OPC UA Server Certificates	admin
	Modbus		Modbus Services Configuration	user
Security				
	OpenVPN / IPsec		OpenVPN / IPsec Configuration	admin
	Firewall			
		General Configuration	General Firewall Configuration	admin
		Interface Configuration	Interface Configuration	admin
		MAC Address Filter	Configuration of MAC Address Filter	admin
		User Filter	Configuration of User Filter	admin
	Certificates		Certificates	admin
	TLS		Security Settings	admin
	Integrity		Advanced Intrusion Detection Environment (AIDE)	admin
Diagnostic			Diagnostic Information	guest

8.8.1.2 General Information about the Page

The IP address of the active device is displayed in the entry line of the browser window.

The WBM pages are only displayed after logging in. To log in, enter your username and password in the login window and click the **[Login]** button.

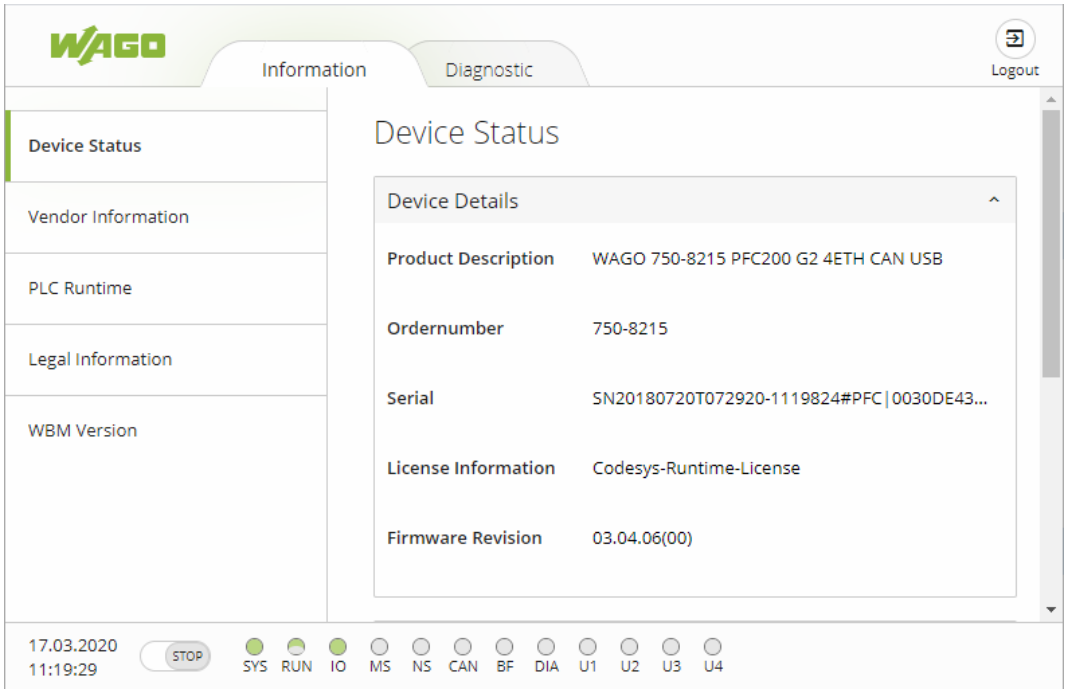


Figure 33: WBM Browser Window (Example)

The tabs for the various WBM areas and the **[Reboot]** and **[Logout]** buttons are displayed in the header of the browser window. The **[Reboot]** button only appears if you are logged in as an administrator.

If not all tabs can be displayed in the selected width of the window, a tab with ellipsis (...) is displayed instead of the tabs that cannot be displayed. This allows you to select the tabs (not shown) using a pull-down menu.

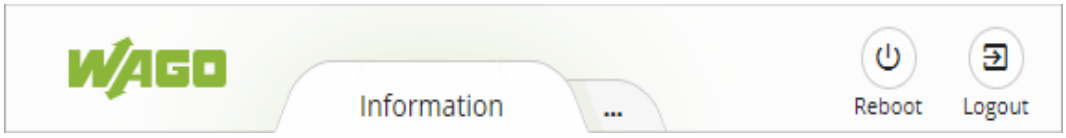


Figure 34: WBM Header with Tabs that Cannot be Displayed (Example)

The navigation tree is shown on the left of the browser window. The content of the navigation tree depends on the selected tab.
You can use this navigation tree to go to the individual pages and, where provided, subpages included in these pages.

The current device status is displayed in the status bar.

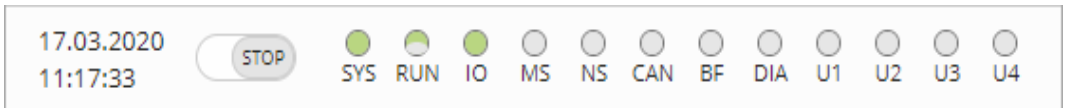


Figure 35: WBM Status Bar (Example)

- Date and Time - Local date and local time and on the device
- Setting of the mode selector switch
- LED status of the Device:
  All LEDs are graphically represented and are labeled with their particular designation (e.g., SYS, RUN, …). The following colors are possible:

  - gray: LED is off.
  - full color (green, red, yellow, orange): The LED is activated in the particular color.
  - half color:
    The LED is flashing in the corresponding color. The other half of the surface is then either gray or also colored. The latter case indicates that the LED is flashing sequentially in different colors.

  A tooltip containing more detailed information opens as long as the cursor is positioned over an LED. The text that is displayed also contains the message that put the LED into its current status. The time of the message is also shown.
  The states displayed in the WBM will not always correspond at the precise time to those on the controller. Data has a runtime during transmission and can only be queried at a certain interval. The time period between two queries is 30 seconds.

Note

Do not power cycle the controller after changing any parameters!
Some parameter changes require a controller restart for the changes to apply. Saving changes takes time.
Do not power cycle the controller to perform a restart, i.e., changes may be lost by shutting down the controller too soon.
Only restart the controller using the software reboot function. This ensures that all memory operations are completed correctly and completely.

A description of the WBM pages and the respective parameters can be found in the appendix in Section “Configuration Dialogs” > “Web-Based Management (WBM)”.

8.8.2 Configuration via Console-Based-Management-Tool (CBM) using a Terminal Program

The Console-Based Management Tool (CBM) is basically used for the initial configuration and startup of the controller via a terminal program.
Therefore, it only provides a subset of the controller parameters. For example, parameters that cannot be displayed in a terminal window in a reasonable way and are not necessary for initial startup are not displayed.

1. Connect a PC to the ETHERNET interface X1 of the controller using an SSH terminal program.

2. Start the terminal program.

3. Select “SSH” as the connection type, and enter the IP address of the controller and port 22 as the connection parameters.

4. Log in to the Linux® system as a “super user.”
The user name and the password are provided in the Section “Users and Passwords” > “Linux® User Group.”

5. Start the configuration tool by entering the command “cbm” (case sensitive) on the command line and then press **[Enter]**.

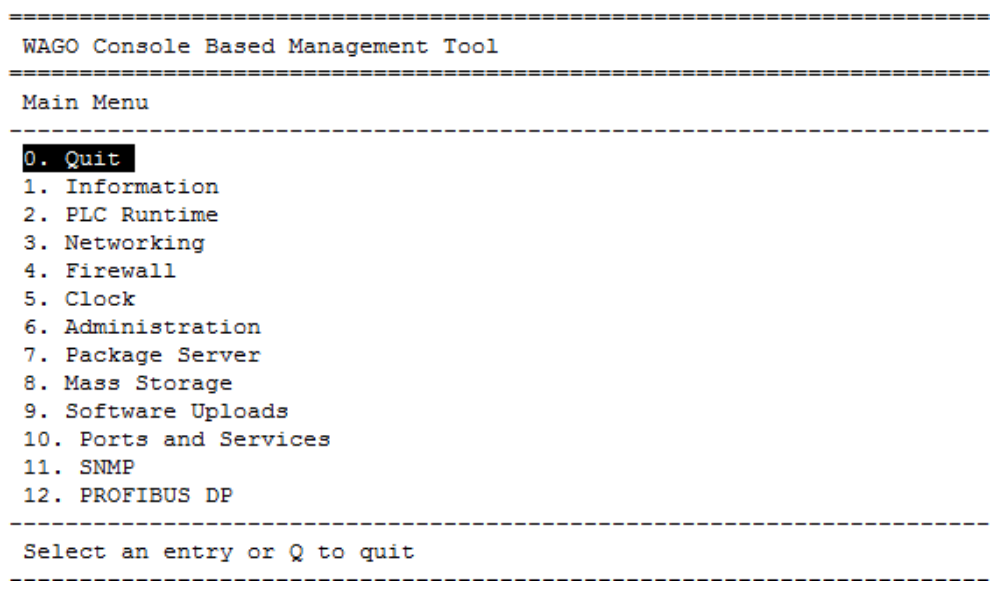


Figure 36: CBM main menu (example)

8.8.2.1 CBM Menu Structure Overview

Table 35: CBM Menu Structure

Menu Hierarchy
0. Quit
1. Information
0. Back to Main Menu
1. Controller Details
2. Network Details
2. PLC Runtime
0. Back to Main Menu
1. Information
2. General Configuration
3. WebVisu
3. Networking
0. Back to Main Menu
1. Host-/Domain Name
2. TCP/IP
0. Back to Networking Menu
1. IP Address
2. Default Gateway
3. DNS Server
3. Ethernet
0. Back to Networking Menu
1. Switch Configuration
2. Ethernet Ports
0. Back to Ethernet Menu
1. Interface X1
2. Interface X2
4. Firewall
0. Back to Main Menu
1. General Configuration
2. MAC Address Filter
3. User Filter
5. Clock
0. Back to Main Menu
1. Date on device (local)
2. Time on device (local)
3. Time on device (UTC)
4. Clock Display Mode
5. Timezone
6. TZ-String
6. Administration
0. Back to Main Menu

Table 35: CBM Menu Structure

Menu Hierarchy
1. Users
2. Create Image
3. Reboot Controller
7. Package Server
0. Back to Main Menu
1. Firmware Backup
2. Firmware Restore
3. System Partition
8. Mass Storage
0. Back to Main Menu
1. Internal Flash (active partition)
9. Software Uploads
0. Back to Main Menu
1. Update Script
10. Ports and Services
0. Back to Main Menu
1. Telnet
2. FTP
3. FTPS
4. HTTP
5. HTTPS
6. NTP
7. SSH
8. TFTP
9. DHCPD
10. DNS
11. IOCHECK PORT
12. Modbus TCP
13. Modbus UDP
14. PLC Runtime Services
11. SNMP
0. Back to Main Menu
1. General SNMP Configuration
2. SNMP v1/v2c Manager Configuration
3. SNMP v1/v2c Trap Receiver Configuration
4. SNMP v3 Configuration
5. SNMP firewalling
6. Secure SNMP firewalling



Note

Do not power cycle the controller after changing any parameters!
Some parameter changes require a controller restart for the changes to apply. Saving changes takes time.
Do not power cycle the controller to perform a restart, i.e., changes may be lost by shutting down the controller too soon.
Only restart the controller using the software reboot function. This ensures that all memory operations are completed correctly and completely.

A description of the CBM menus and the respective parameters can be found in the appendix in Section “Configuration Dialogs” > “Console-Based Management (CBM)”.

8.8.3 Configuration using “WAGO Ethernet Settings”

The “WAGO Ethernet Settings” program enables you to read system information about your controller, make network settings and enable/disable the Web server.

Note

Observe the software version!
To configure the controller, use at least Version 6.4.1.1 dated 2015-06-29 or newer of “WAGO Ethernet Settings”!

You must select the corresponding interface after launching the “WAGO ETHERNET Settings”.

A connection can be established via the service interface using communication cable 750-920, *Bluetooth*® Adapter 750-921, configuration cable 750-923 or 750-923/000-001 or via the ETHERNET interfaces.

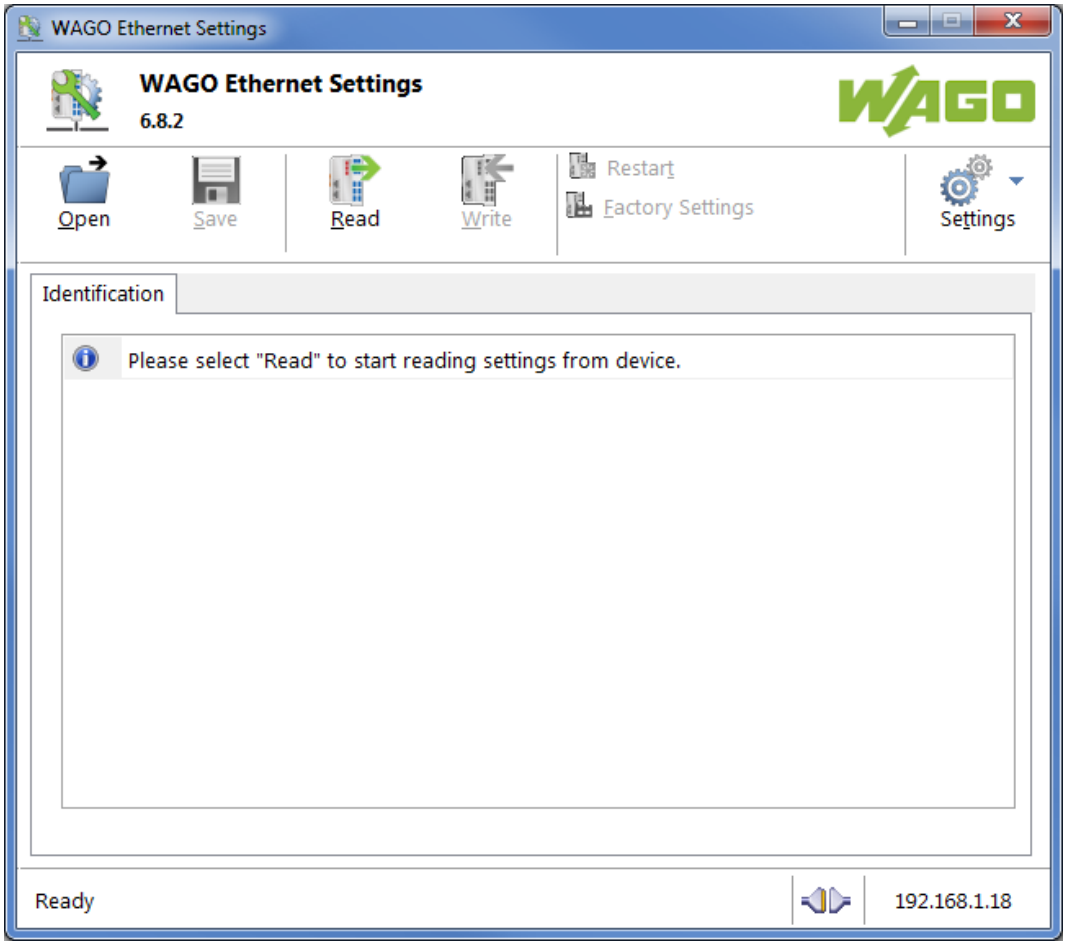


Figure 37: “WAGO Ethernet Settings” – Start Screen

For this, click “Settings” and then “Communication”.

In the “Communication settings” window that then opens, adapt the settings to your needs.

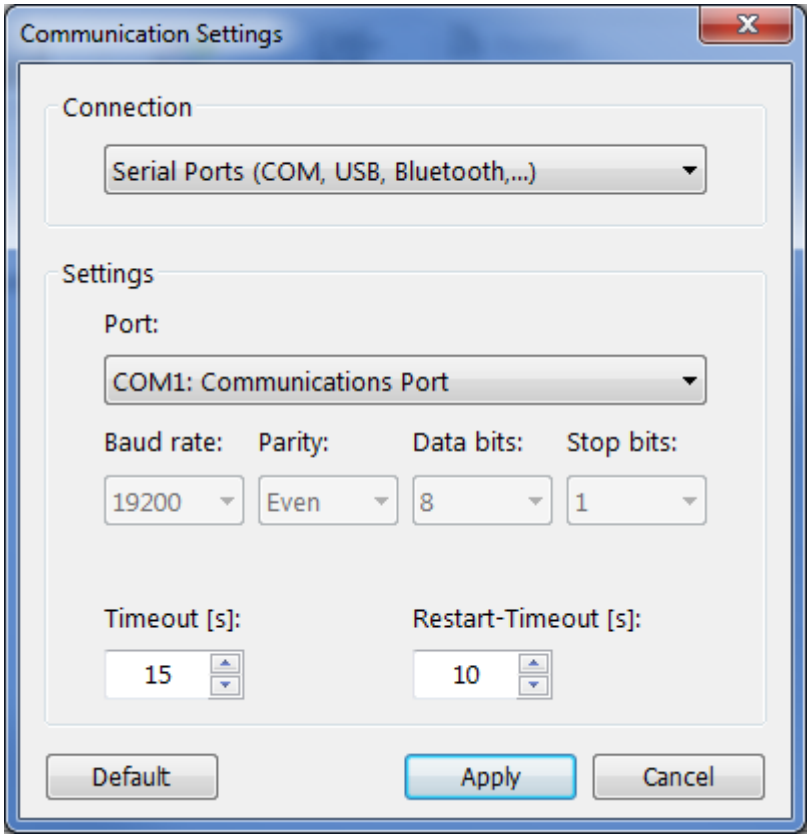


Figure 38: “WAGO Ethernet Settings” – Communication Link

Once you have configured “WAGO Ethernet Settings” and have clicked **[Apply]**, connection to the controller is established automatically.

If “WAGO Ethernet Settings” has already been started with the correct parameters, you can establish connection to the controller by clicking **[Read]**.

8.8.3.1 Identification Tab

An overview of the connected device is given here.

Besides some fixed values — e.g., item No., MAC address and firmware version — the currently used IP address and the configuration method are also shown here.

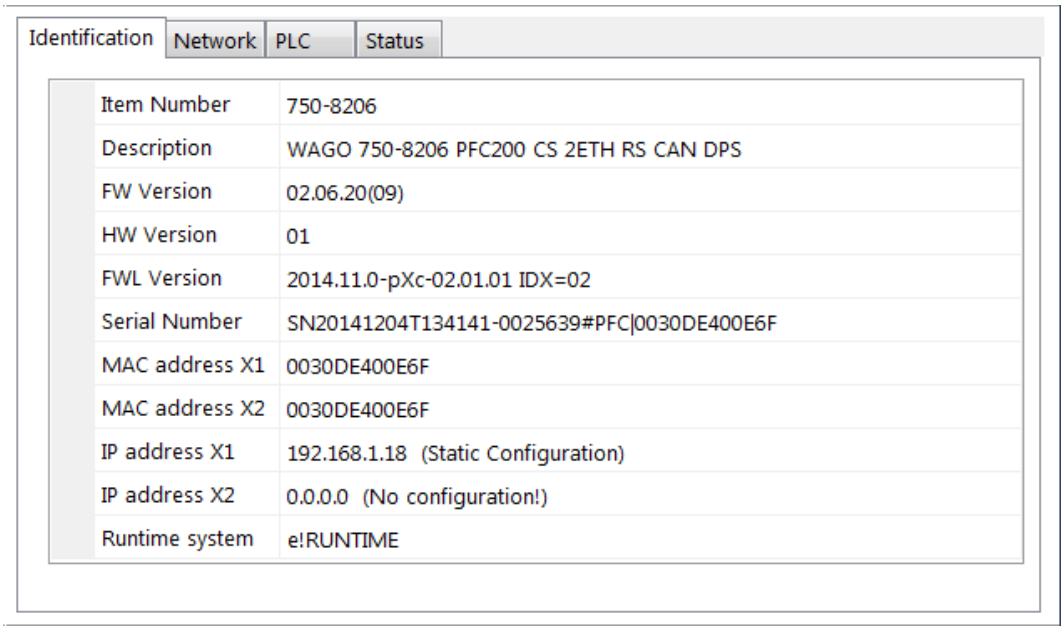


Figure 39: “WAGO Ethernet Settings” – Identification Tab (Example)

8.8.3.2 Network Tab

This tab is used to configure network settings.

Values can be changed in the “Input” column, while the parameters in use are shown in the “Currently in use” column.

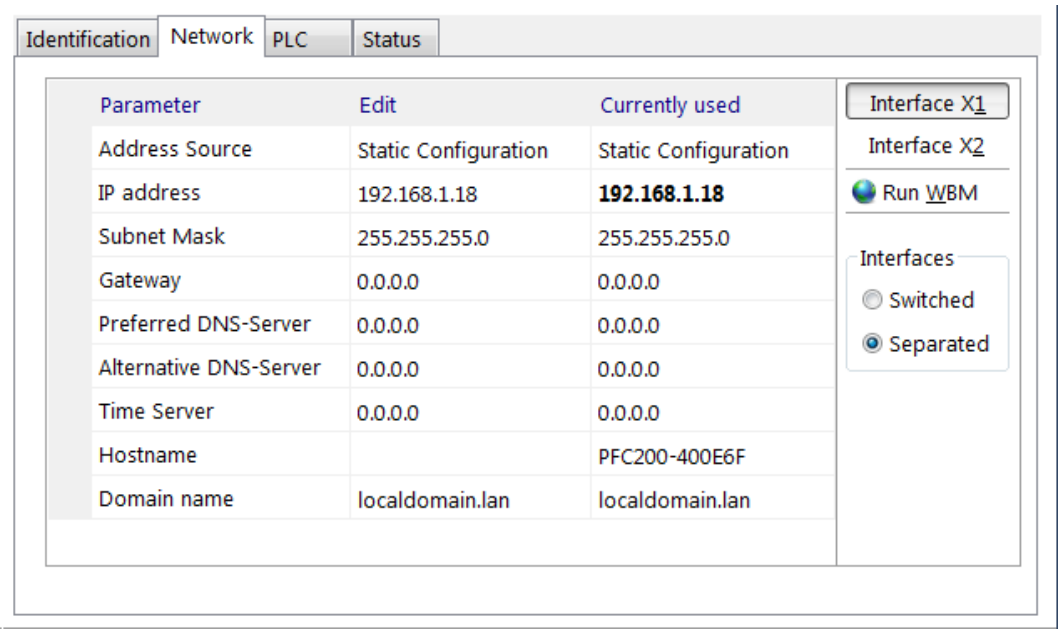


Figure 40: “WAGO Ethernet Settings” – Network Tab

Address Source
Specify how the controller will determine its IP address: Static, via DHCP or via BootP.

IP address, subnet mask, gateway
Specify the specific network parameters for static configuration.

Note

Restricted setting for default gateways!
Only the default gateway 1 can be set via “WAGO Ethernet Settings.”
The default gateway 2 can only be set in the WBM!

Preferred DNS server, alternative DNS server
Enter the IP address (when required) for an accessible DNS server when identifying network names.

Time server
Specify the IP address for a time server if setting the controller's system time via NTP.

Hostname
The host name of the controller is displayed here. In the controller's initial state, this name is composed of the string “PFCx00” and the last three bytes of the

MAC address.
This standard value is also used whenever the chosen name in the “Input” column is deleted.

Domain name
The current domain name is displayed here. This setting can be automatically overwritten with dynamic configurations, e.g., DHCP.

8.8.3.3 PLC Tab

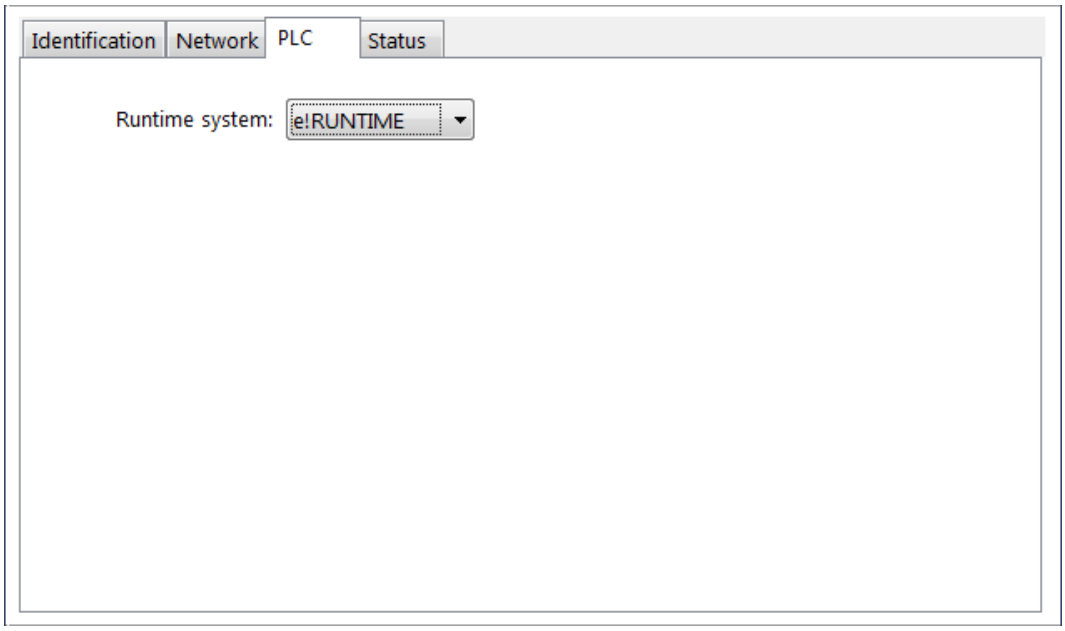


Figure 41: “WAGO Ethernet Settings” – Protocol Tab

Here you can select the runtime system.

8.8.3.4 Status Tab

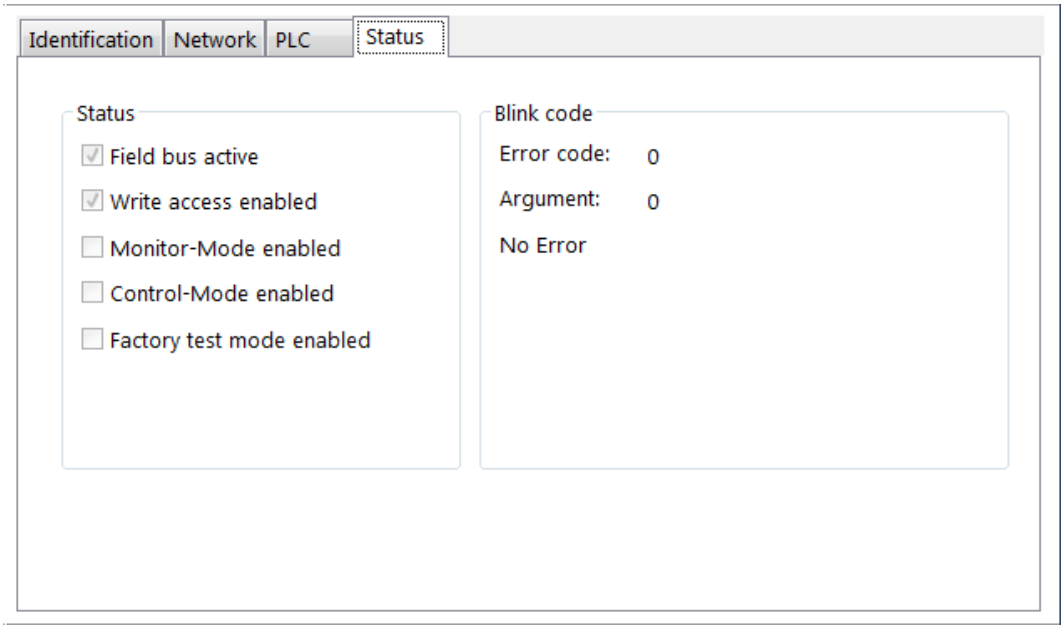


Figure 42: “WAGO Ethernet Settings” – Status Tab

General information about the controller status is displayed here.

9 *e!RUNTIME* Runtime Environment

9.1 General Notes



Note

Additional Information
Information on the installation and startup of ***e!****COCKPIT* is provided in the corresponding manual.
Information on programming is provided in the CODESYS 3 documentation.

9.2 CODESYS V3 Priorities

A list of priorities implemented for the controller is provided below as supplementary information to the CODESYS 3 documentation.

Table 36: CODESYS V3 Priorities

Scheduler	Task	Linux® Priority	IEC Priority	Remark
Preemptive scheduling - Real-time range	Local bus or fieldbus - HIGH	-95 … -86		Local bus (-88)
	Mode selector switch monitoring	-85		Task registers changes to the mode selector switch and changes the state of the PLC application. (start, stop, reset warm/cold)
	CODESYS watchdog	-83		Execution of the watchdog functions
	Cyclic and event-controlled IEC task	-55 … -53	1 … 3	For real-time tasks which must not be influenced in execution by external interfaces (e.g., fieldbus).
	Local bus or fieldbus - MID	-52 … -43		CAN (-52 … -51) PROFIBUS (-49 … -45) Modbus® slave/master (-43)
	Cyclic and event-controlled IEC task	-42 … -32	4 … 14	For real-time tasks which must not influence fieldbus communication during execution.
	Local bus or fieldbus – LOW	-13 … -4		
Fair scheduling - None real-time range	CODESYS communication	Back-ground (20)		Communication with the CODESYS development environment
	Cyclic, event-controlled and freewheeling IEC task		15	Incl. standard priority of the visualization task

9.3 Memory Spaces under *e!RUNTIME*

The memory spaces in the controller under ***e!****RUNTIME* have the following sizes:

- Program and data memory: 10 Mbytes
- Input data: 64 kbytes
- Output data: 64 kbytes
- Flags: 12 kbytes
- Retain: 52 kbytes
- Function block limitation: 12 * 4096 bytes = 48 kbytes

9.3.1 Program and Data Memory

The program (also code) and data memory has a size of 10 Mbytes.
This space has already been requested in the system after a successful program download and can be fully utilized.
The memory space is dynamically divided up into program and data space.

9.3.2 Function Block Limitation

Together with the data memory to be used by the application, memory is required for the individual program function blocks in the system.

The size of the administration space is calculated from the function block limitation * 12 (i.e., 4096 Byte * 12).

The actual size of the main memory required in the system for data is the sum of global program and data memory and function block limitation memory.

9.3.3 Remanent Memory

A total of 64 kbytes of remanent memory is available for the IEC-61131 application.
The remanent section is subdivided into the flag area (memory) and the retain area.

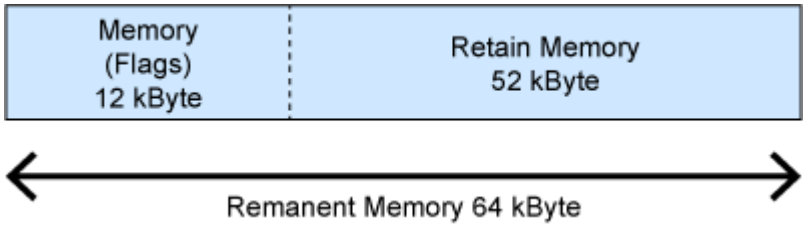


Figure 43: Remanent Main Memory

10 Modbus – *e!RUNTIME*

10.1 Modbus Address Overview

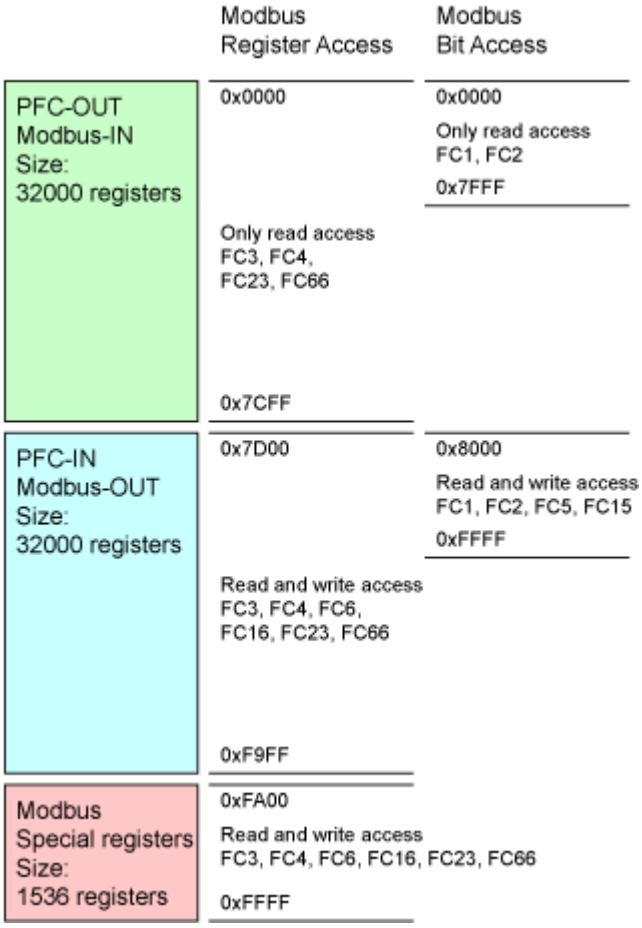


Figure 44: Modbus Address Overview

10.2 Modbus Registers

Table 37: WAGO Modbus Registers

Modbus Address		Data Length in Words	Access	Description
Dec.	Hex.			
Watchdog Configuration Registers				
64,000	0xFA00	1	w	Watchdog command register
64,001	0xFA01	1	rw	Watchdog timeout register
64,002	0xFA02	1	ro	Watchdog status register
64,003	0xFA03	1	rw	Watchdog config register
64,004	0xFA04	1	rw	Modbus TCP connection watchdog register
Status Registers				
64,010	0xFA0A	1	ro	LED flash code I/O-LED (sequence 1 of 3)
64,011	0xFA0B	1	ro	LED flash code I/O-LED (sequence 2 of 3)
64,012	0xFA0C	1	ro	LED flash code I/O-LED (sequence 3 of 3)
64,013	0xFA0D	1	ro	PLC State : 1 = Stop; 2 = Run
Electronic Type Label				
64,016	0xFA10	4	ro	Order number, e.g., 0750810100400001
64,020	0xFA14	1	ro	Firmware status
64,021	0xFA15	1	ro	Hardware version
64,022	0xFA16	1	ro	Firmware loader
Process Image Version				
64,023	0xFA17	1	ro	Version of the Modbus process image
Network Configuration				
64,032	0xFA20	3	ro	MAC-ID 1
Process Image Registers				
64,064	0xFA40	1	ro	Number of input registers, analog and digital (total size of the Modbus IN space) 0x7D00
64,065	0xFA41	1	ro	Number of input registers, analog 0x7D00
64,066	0xFA42	1	ro	Number of input registers, digital 0x8000
64,067	0xFA43	1	ro	Number of output registers, analog and digital (total size of the Modbus OUT space) 0x7D00
64,068	0xFA44	1	ro	Number of output registers, analog 0x7D00
64,069	0xFA45	1	ro	Number of output registers, digital 0x8000

Table 37: WAGO Modbus Registers

Modbus Address		Data Length in Words	Access	Description
Dec.	Hex.			
Constants Registers				
64,160	0xFAA0	1	ro	Constant 0x1234
64,161	0xFAA1	1	ro	Constant 0xAAAA
64,162	0xFAA2	1	ro	Constant 0x5555
64,250	0xFAFA	1	ro	Live register

The WAGO Modbus registers are described in more details in the following sections.

10.2.1 Modbus Watchdog

The Modbus watchdog monitors in the Modbus slave the ongoing Modbus communication with the Modbus master. All valid Modbus requests of a Modbus master from all the services supported by the Modbus slave are trigger events (see chapter “Modbus Mapping”). Exceptions here are the Explicit Trigger mode and the access to the register 0xFA02 (Watchdog Status), which can be configured via the register 0xFA03 (Watchdog Config).

The “Watchdog Timeout” response is initiated if no trigger occurs within the timeout set in the register 0xFA01 (Watchdog Timeout) with the watchdog running. The closing of all Modbus TCP connections can be configured as a response, see register 0xFA03 (Watchdog Config).

The Modbus watchdog supports two different operation modes ADVANCED_WATCHDOG and SIMPLE_WATCHDOG. The operation mode can be selected via Bit 7 in the register 0xFA03 (Watchdog Config).

The following diagrams show the possible states of the Modbus watchdog and status transitions for the particular operation mode.

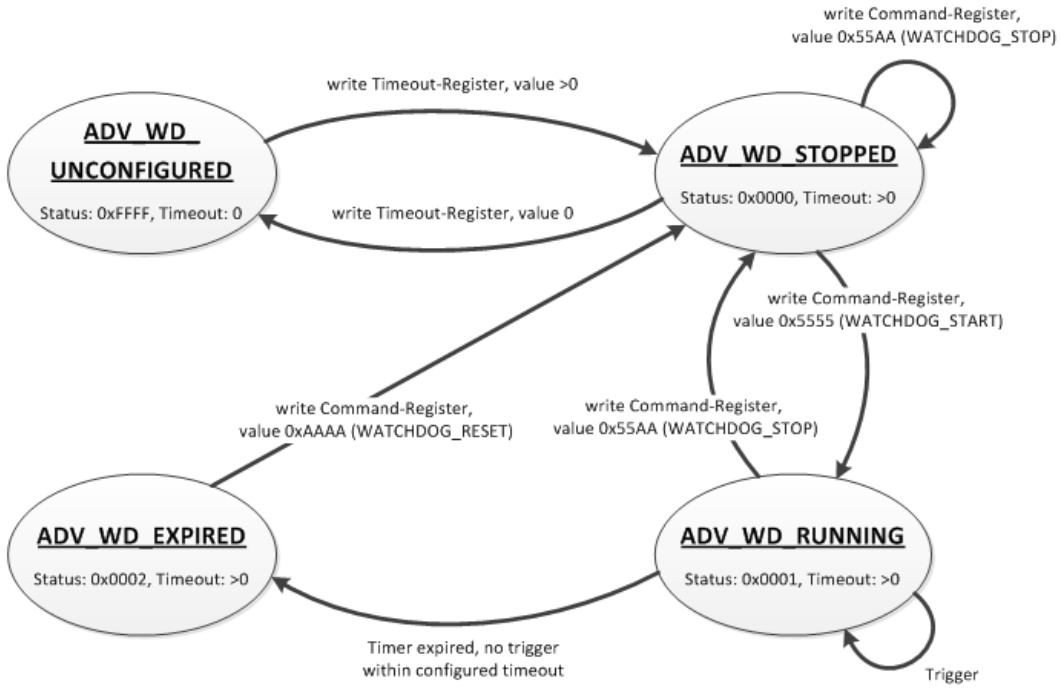


Figure 45: State Diagram, ADVANCED_WATCHDOG Operation Mode

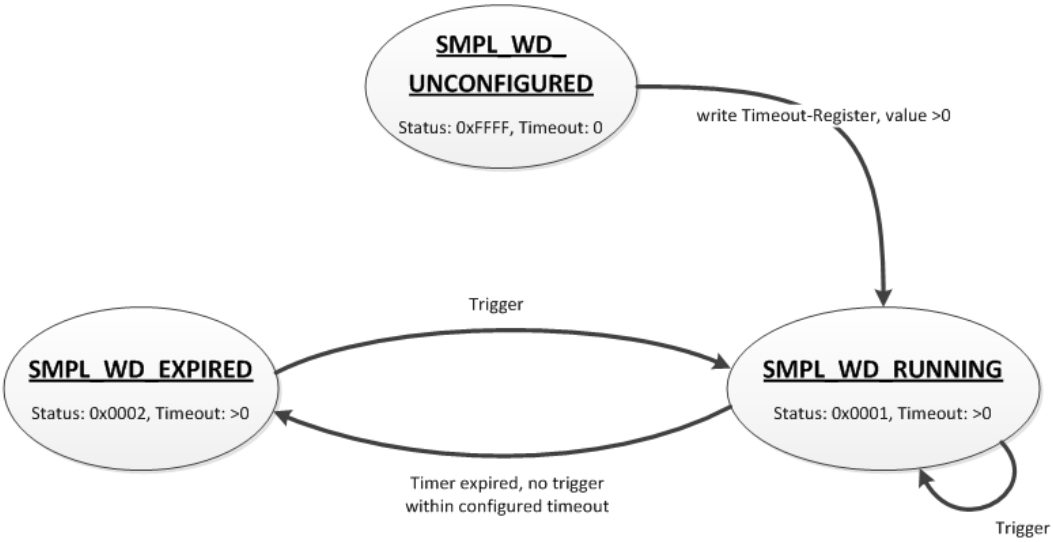


Figure 46: State Diagram, SIMPLE_WATCHDOG Operation Mode

The state diagram for the SIMPLE_WATCHDOG operation mode shows that the watchdog is always active as soon as a timeout > 0 is set in the register 0xFA01 (Watchdog Timeout). The writing of commands in the register 0xFA00 (Watchdog Command) is restricted in this operation mode. Only the WATCHDOG_START command is permitted as a possible trigger. The only possibility to deactivate and stop the watchdog in operation mode SIMPLE_WATCHDOG, is the switching back to the operation mode ADVANCED_WATCHDOG.

The following diagram shows the possible state transitions when operation modes are switched.

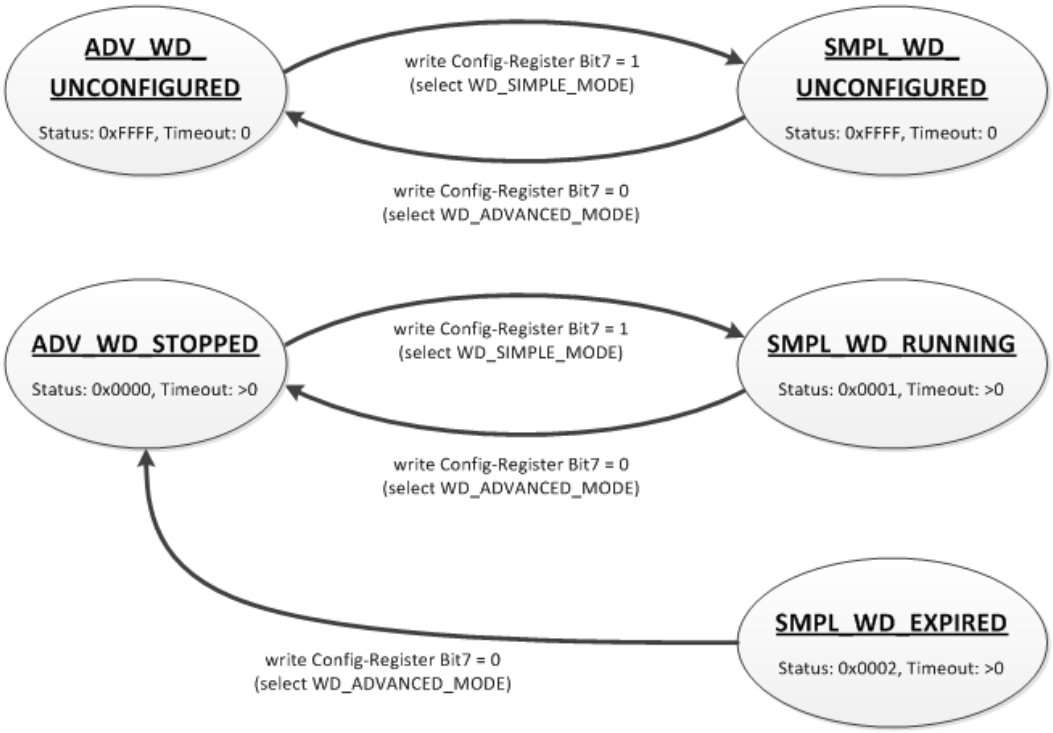


Figure 47: State Diagram, Switching Operation Modes

10.2.1.1 Register 0xFA00 – Watchdog Command

This register receives commands for the Modbus watchdog. It cannot be read, i.e. it is not possible to read out the last command written.
The following commands are accepted depending on watchdog status:

Table 38: Watchdog Commands

Value	Name	Explanation
0x5555	WATCHDOG_ START	Starts the configured watchdog; in the WATCHDOG_UNCONFIGURED state if no timeout is configured, the response is an ILLEGAL_DATA_VALUE (0x03) exception. The same exception is returned even if the watchdog has expired (WATCHDOG_EXPIRED) in the ADVANCED_ WATCHDOG operation mode. The watchdog must in this case be reset first with the command WATCHDOG_RESET to the WATCHDOG_STOPPED state. In all other cases the watchdog is restarted and the WATCHDOG_RUNNING state is set.
0x55AA	WATCHDOG_ STOP	Stops the running watchdog; in the WATCHDOG_UNCONFIGURED state, the response is an ILLEGAL_DATA_ VALUE (0x03) exception if no timeout time is set. The same exception is returned even if the watchdog has expired (WATCHDOG_EXPIRED) in the ADVANCED_ WATCHDOG operation mode. The watchdog must in this case be reset first with the command WATCHDOG_RESET to the WATCHDOG_STOPPED state. In the SIMPLE_ WATCHDOG operation mode the response is an ILLEGAL_DATA_VALUE (0x03) exception. The command is not generally permitted in this operation mode. In all other cases, the watchdog is stopped and the WATCHDOG_STOPPED state is set. In the WATCHDOG_STOPPED state a stop command received several times in a row does not have any impact on the behavior of the watchdog and is therefore not acknowledged with an error response.
0xAAAA	WATCHDOG_ RESET	Resets the expired watchdog; in the WATCHDOG_EXPIRED state the ADVANCED_WATCHDOG operation mode resets the watchdog. The watchdog is then in the WATCHDOG_STOPPED state. In all other cases the response is an ILLEGAL_ DATA_VALUE (0x03) exception.

10.2.1.2 Register 0xFA01 – Watchdog Timeout

This register contains the value for the watchdog timeout. The step width is 1 ms and the maximum value is 65535 (corresponds to 65.535 s). The default value is 0. In this case the watchdog cannot be started and will have the WATCHDOG_UNCONFIGURED state.

The register can be read and written in the states WATCHDOG_UNCONFIGURED and WATCHDOG_STOPPED. However, if the watchdog is active or expired (WATCHDOG_RUNNING and WATCHDOG_EXPIRED state), only read access to this register is possible. The response to a write operation is an ILLEGAL_FUNCTION (0x01) exception.

10.2.1.3 Register 0xFA02 – Watchdog Status

This register provides the current state of the Modbus watchdog.
The following states are possible:

Table 39: Watchdog Status

Value	Name	Explanation
0xFFFF	WATCHDOG_ UNCONFIGURED	The Modbus watchdog is not configured, i.e., register 0xFA01 (Watchdog Timeout) contains the value 0. Only the setting of a timeout > 0 s can close this state.
0x0000	WATCHDOG_ STOPPED	The Modbus watchdog is configured, the register 0xFA01 (Watchdog Timeout) contains a value >0. In the ADVANCED_WATCHDOG operation mode, the watchdog can be activated in this state with the WATCHDOG_START command. In the SIMPLE_WATCHDOG operation mode, this state cannot be accessed since the watchdog is automatically started.
0x0001	WATCHDOG_ RUNNING	The Modbus watchdog is active, i.e. configured and started. The set timeout has not yet expired.
0x0002	WATCHDOG_ EXPIRED	The timeout set in register 0xFA01 (Watchdog Timeout) has expired. In the ADVANCED_WATCHDOG operation mode, the watchdog in this state must be reset to the WATCHDOG_STOPPED state with the WATCHDOG_RESET command. In the SIMPLE_WATCHDOG operation mode, the watchdog is automatically restarted with the next trigger.

10.2.1.4 Register 0xFA03 – Watchdog Config

This register contains the configuration parameters for the watchdog. The register is organized in bits, see following table.

The register can be read and written irrespective of the watchdog state in the SIMPLE_WATCHDOG operation mode.
However, in the ADVANCED_WATCHDOG operation mode, the register can only be read and written in the WATCHDOG_UNCONFIGURED and WATCHDOG_STOPPED states.
If the watchdog is active (WATCHDOG_RUNNING or WATCHDOG_EXPIRED state), only a read access is permissible. The response to a write request in this case is an ILLEGAL_FUNCTION (0x01) exception.

Table 40: Watchdog Configuration

Bit	Name/Bit Identifier	Explanation	
0	EXPLICIT_ TRIGGER_ONLY	Activates the Explicit Trigger mode	
		0*	All valid Modbus requests are considered as watchdog triggers. Access to register 0xFA02 (Watchdog Status) is the only exception.
		1	Only the writing of register 0xFA00 (Watchdog Command) with the value 0x5555 (WATCHDOG_START) is considered as the watchdog trigger. The exception is also here the access to the register 0xFA02 (Watchdog Status).
1	TRIGGER_ON_ STATUS_REG	Activates the watchdog trigger by (read) access to register 0xFA02 (Watchdog Status)	
		0*	The reading of the watchdog status is not considered as a watchdog trigger.
		1	The reading of the watchdog status triggers the watchdog.
2	CLOSE_ALL_TCP_ CONNECTIONS	Activates the closing of all Modbus TCP connections with the expiry of the timeout (transition to WATCHDOG_EXPIRED state)	
		0	Existing Modbus TCP connections remain open.
		1*	All existing Modbus TCP connections are closed.
7	SELECT_ ADVANCED_ SIMPLE_MODE	Determines the watchdog operation mode	
		0*	Advanced Mode: The watchdog must be controlled explicitly via commands (see register 0xFA00 Watchdog Command).
		1	Simple Mode: The watchdog is activated directly with a timeout > 0 in register 0xFA01 (Watchdog Timeout). Each trigger restarts the running as well as the expired watchdog. The watchdog can only be stopped by switching to Advanced mode.
*Default setting			

The individual options are activated if the relevant bit or bit combination is set.

10.2.1.5 Modbus TCP Connection Watchdog Register

The 0xFA04 register contains the time for the Modbus TCP connection watchdog. Time base is 10 ms. This enables the time to be set up to 655350 ms. If the register contains a value > 0 s when a new TCP connection from a Modbus master is accepted, the watchdog for this connection is started. Later changes to the register have no effect on the monitoring of existing connections. If the watchdog is started and no telegram is received from the connected Modbus master within the set time, this connection is closed from one side with a reset.

10.2.2 Status Registers

10.2.2.1 PLC Status Register

The register 0xFA0D supplies the current status of the controller.
Possible values:

1 = PLC Stop - PLC is in STOP status.
2 = PLC Run - PLC is in RUN status

10.2.3 Electronic Nameplate

Registers 0xFA10–0xFA17 contain information from the electronic nameplate. It is possible to read the entire nameplate or a consecutive portion of it all at once.

10.2.3.1 Order Number

The registers 0xFA10–0xFA13 contain the WAGO order number of the controller.

Example: 0750-8202/0025-0001.

0xFA10 = 0750,
0xFA11 = 8202,
0xFA12 = 0025,
0xFA13 = 0001

10.2.3.2 Firmware Version

The register 0xFA14 contains the firmware version of the controller.

10.2.3.3 Hardware Version

The register 0xFA15 contains the hardware version of the controller.

10.2.3.4 Firmware Loader/Boot Loader

The register 0xFA16 contains the firmware loader/boot loader version of the controller.

10.2.4 Modbus Process Image Version

The register 0xFA17 contains the Modbus process image version of the controller.

10.2.5 Modbus Process Image Registers

The registers 0xFA40–0xFA45 contain size information for the process image spaces of the controller for bit and register accesses.

10.2.6 Constant Registers

Registers 0xFAA0 … 0xFAA2 provide constants based on the “WAGO Modbus Registers” table. It is possible to read all of the constants, or a consecutive portion of them at once.

0xFAA0 = 0x1234,
0xFAA1 = 0xAAAA,
0xFAA2 = 0x5555

10.2.7 Live Register

The register 0xFAFA can only be read and contains a counter that is incremented with each cycle of a task of the runtime environment with read and write access to the Modbus process data.

10.3 Estimating the Modbus Master CPU Load

Due to the real-time characteristics of the Linux kernel used, many data points can generate many context changes.
For a one-off update (transmitting and receiving of a function code), a CPU time of approx. 800 µs can be assumed.
The CPU load (cpu_load) in percent can be estimated from the cycle time (t_z) for a query with the following rule of thumb:

cpu_load = 800 µs / t_z * 100

A cycle time of 100 ms thus results in a CPU load of 0.8%.
A maximum load of approx. 20% can be generated per connection, as this is limited by the network protocol. To minimize the CPU load:

- The cycle time must be as high as possible.
- As many data points as possible must be combined in a query.
- The minimum query interval can be increased (default value: 0 ms).

11 Diagnostics

11.1 Operating and Status Messages

The following tables contain descriptions of all operating and status messages for the controller which are indicated by LEDs.

11.1.1 System/Fieldbus LEDs



Figure 48: Indicating elements for fieldbus/system

11.1.1.1 SYS LED

The SYS LED indicates following diagnostics:

Table 41: Diagnostics via SYS LED

Status	Explanation	Remedy
Green	Ready to operate - System start completed without errors	---
Orange	Device is in startup/boot process and the RST button is not pressed.	---
Orange flashing	“Fix IP Address” mode, temporary setting until the next reboot	Connect to the device via the standard address (192.168.1.17) or restart the device to restore the original value set.
Green/red flashing	Firmware update mode	---

11.1.1.2 RUN LED

The RUN LED indicates following diagnostics:

Table 42: RUN LED Diagnostics

Status	Explanation	Remedy
Green	Applications loaded and all in the “RUN” status	---
Green flashing	No application and now boot project loaded	Load an application or boot project.
Red	Applications loaded and all in the “STOP” status	Set the mode selector switch to “RUN” to start the application.
Green/red flashing	At least one application in the “RUN” status and one in the ”STOP” status	Start the stopped application.
Red, goes out briefly	Warm start reset completed	---
Red, goes out longer	Cold start reset completed	---
Red, flashing	At least one application after in the “STOP” status after exception (e.g., memory access error)	Start the application with a reset via the mode selector switch or in the connected IDE. If the application cannot be started, restart the controller. Contact WAGO Support if the error occurs again.
Orange/green flashing	Load above threshold value 1	Try to reduce the load on the system: - Change the CODESYS program. - End any fieldbus communication that is not essential, or reconfigure the fieldbuses. - Remove any non-critical tasks from the RT area. - Select a longer cycle time for IEC tasks.
Orange	Runtime system in debug state (breakpoint, single step, individual cycle)	Resume the application in the connected IDE with single step or start. Remove the breakpoint if necessary. If the connection has been interrupted, set the mode selector switch to “STOP” and then back to “RUN” to enable the application to continue
OFF	No runtime system loaded	Enable a runtime system, e.g., via the WBM.

11.1.1.3 I/O LED

The I/O LED indicates following diagnostics:

Table 43: Diagnostics I/O LED

Status	Explanation	Solution
Green	Data cycle on the local bus, normal operating status.	---
Orange flashing	Startup phase; the local bus is being initialized. The startup phase is indicated by rapid flashing for about 1 ... 2 seconds.	Wait until initialization has been completed.
Red	A hardware fault is present.	Contact WAGO Support.
Red flashing (2 Hz)	An error which may be able to be eliminated is present.	First, try to eliminate the error by switching the device (power supply) off and then back on. Check the entire node structure for any errors. If you cannot eliminate the error, contact WAGO Support.
Red flashing (flashing sequence)	A local bus error is present.	An explanation of the flashing sequence is given in the section “Diagnostics Messages via Flashing Sequences”.
Off	A library was not loaded, or a library function was not called up.	Restart the device. If you cannot eliminate the error, contact WAGO Support.

11.1.1.4 MS LED

The MS LED indicates following diagnostics:

Table 44: MS-LED Diagnostics

Status	Explanation	Remedy
Off	No error	---
Red flashing (flashing sequence)	A configuration error exists.	An explanation of the flashing sequence is given in the section “Diagnostics via Flashing Sequences.”

11.1.2 Network Connection LEDs

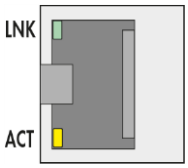


Figure 49: Indicating Elements, RJ-45 Jacks

11.1.2.1 LNK LED

The LNK LED indicates following diagnostics:

Table 45: LNK-LED Diagnostics

Status	Explanation	Remedy
Off	10 Mbit/s	---
Green	100 Mbit/s	---

11.1.2.2 ACT LED

The ACT LED indicates following diagnostics:

Table 46: ACT-LED Diagnostics

Status	Explanation	Remedy
Off	No network communication via port	Check network connections and network settings.
Yellow flashing	Network communication via port	---

11.1.3 Memory Card Slot LED

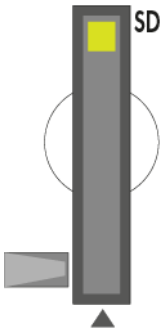


Figure 50: Indicating Elements, Memory Card Slot

The memory card slot LED indicates following diagnostics:

Table 47: Diagnostics via Memory Card Slot LED

Status	Explanation	Remedy
Off	No memory card access	---
Yellow	Memory card access	---
Yellow flashing		

11.2 Diagnostics Messages via Flashing Sequences

11.2.1 Flashing Sequences

A diagnosis (fault/error) is always displayed as three flashing sequences in a cyclic manner:

1. The first flashing sequence (flickering) initiates reporting of the fault/error.

2. After a short break (approx. 1 second), the second flashing sequence starts. The number of blink pulses indicates the **error code**, which describes the type of error involved.

3. After a further break the third flashing sequence is initiated. The number of blink pulses indicates the **error argument**, which provides an additional description of the error, e.g., which of the I/O modules connected to the controller exhibits an error.

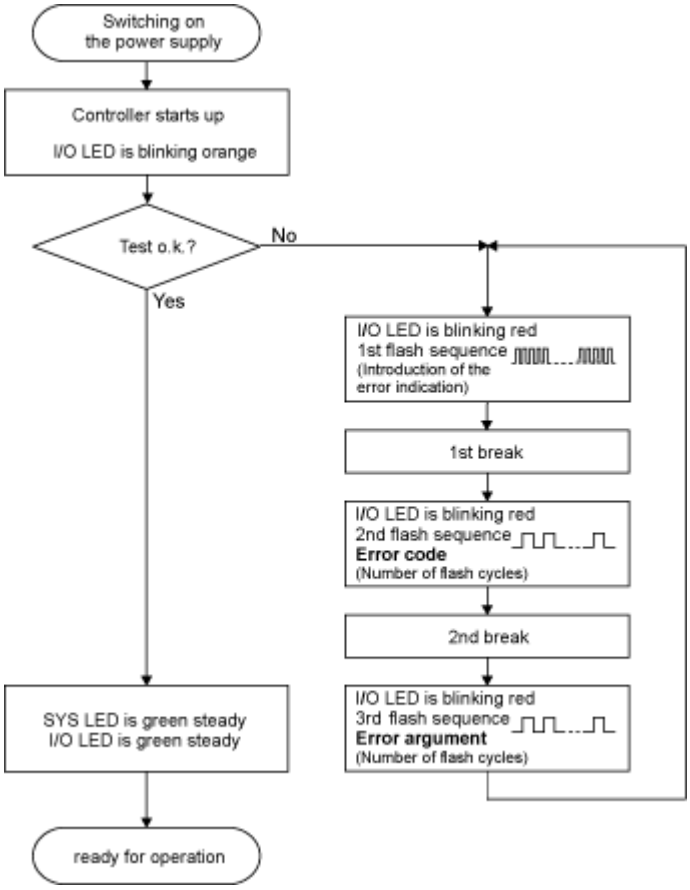


Figure 51: Flashing Sequence Process Diagram

11.2.2 Example of a Diagnostics Message Indicated by a Flashing Sequence

The example below illustrates the representation of a diagnostics message via a flashing sequence. The I/O LED indicates a data error on the local bus. The data error is caused by the removal of an I/O module located at the 6th position of the bus node.

Initiation of the Start Phase

1. The I/O LED flashes for 1 cycle at about 10 Hz (10 flashes/second).

2. This is followed by a pause of about one second.

Error Code 4: Data Error in the Local Bus

3. The I/O LED flashes for 4 cycles of about 1Hz.

4. This is followed by a pause of about 1 second.

Error Argument 5: I/O Module at the 6th Slot

5. The I/O LED flashes for 5 cycles at 1 Hz.
   This indicates that a disruption has occurred at the local bus downcircuit of the 5th I/O module.

6. The blink code starts flickering when the start phase is initiated again. If there is only one error, this process is repeated.

11.2.3 Meaning of Blink Codes and Procedures for Troubleshooting

This section describes the diagnostics presented as blink codes via the I/O LEDs.

If the diagnostics cannot be cleared by the measured specified for them, contact WAGO support. Be ready to explain to them the blink code that is displayed.

Phone: +49 571 887 44 55 5
Fax: +49 571 887 84 45 55
E-mail: support@wago.com

Table 48: Overview of Error Codes, I/O LED

Error code	Explanation
1	Hardware and configuration error
2	Configuration error
3	Local bus protocol error
4	Physical error on the local bus
5	Local bus initialization error
6	Not used
7	Not supported I/O module
8	Not used
9	CPU exception error

Table 49: Error Code 1, Explanation of Blink Codes and Procedures for Troubleshooting

Error Argument	Cause	Remedy
-	Invalid parameter checksum for local bus interface	- Switch off the power to the controller and replace it. - Then switch the power back on.
1	Internal buffer overflow (max. amount of data exceeded) during inline code generation.	- Switch off the power to the controller. - Reduce the number of I/O modules. - Switch the power back on.
2	Data type of the I/O module(s) is not supported	- Update the controller firmware. If this error persists, there is an error in the I/O module. Identify the error as follows: - Switch off the power supply. - Place the end module in the middle of the I/O modules connected to the system. - Switch the power back on. - If the I/O flashes red switch off the power supply again and place the end module in the middle of the first half of the I/O modules (toward the controller). - If the LED is no longer flashing, switch off the power supply and place the end module in the middle of the second half of the I/O modules (away from the controller). - Switch the power back on. - Repeat this procedure until you establish which I/O module is defective. Then replace that module.
3	Unknown module type of the flash program memory	- Switch off the power to the controller and replace it. - Then switch the power back on.
4	Error occurred while writing to the flash memory	- Switch off the power to the controller and replace it. - Then switch the power back on.
5	Error occurred while erasing a flash sector	
6	The I/O module configuration after a local bus reset differs from the one after the last controller startup.	- Restart the controller by first switching off the power supply and then switching it back on, or by pressing the Reset button on the controller.

Table 49: Error Code 1, Explanation of Blink Codes and Procedures for Troubleshooting

Error Argument	Cause	Remedy
7	Error occurred while writing to the serial EEPROM	- Switch off the power to the controller and replace it. - Then switch the power back on.
8	Invalid hardware/ firmware combination	
9	Invalid checksum in the serial EEPROM	
10	Fault when initializing the serial EEPROM.	
11	Error occurred while reading from the serial EEPROM	- Switch off the power supply to the controller and reduce the number of I/O modules. - Then switch the power back on.
12	Time to access the serial EEPROM exceeded	- Switch off the power to the controller and replace it. - Then switch the power back on.
14	Maximum number of gateway or mailbox modules exceeded.	- Switch off the power to the controller. - Reduce the number of gateway or mailbox modules. - Then switch the power back on.
16	Maximum number of I/O modules exceeded	- Switch off the power to the controller. - Reduce the number of I/O modules. - Then switch the power back on.

Table 50: Error Code 2, Explanation of Blink Codes and Procedures for Troubleshooting

Error Argument	Cause	Remedy
2	Maximum size of the process image exceeded	- Switch off the power to the controller. - Reduce the number of I/O modules. - Switch the power back on.

Table 51: Error Code 3, Explanation of Blink Codes and Procedures for Troubleshooting

Error Argument	Cause	Solution
--	Local bus communication error; defective I/O module cannot be identified	If a power supply module (e.g., 750-602) is connected to the controller, ensure that this module functions properly (see Section “LED Signaling”). If the supply module does not exhibit any errors/faults, the I/O module is defective. Identify the defective I/O module as follows: - Switch off the power supply. - Place the end module in the middle of the I/O modules connected to the system. - Switch the power back on. - If the I/O LED continues to flash red switch off the power supply again and place the end module in the middle of the first half of the I/O modules (toward the controller). If only one I/O module is left and the LED continues to flash, either this module or the controller local bus interface is defective. Replace the defective module or the controller. - If the LED is no longer flashing, switch off the power supply and place the end module in the middle of the second half of the I/O modules (away from the controller). - Switch the power back on. - Repeat this procedure until you establish which I/O module is defective. Then replace that module.

Table 52: Error Code 4, Explanation of Blink Codes and Procedures for Troubleshooting

Error Argument	Cause	Solution
--	Maximum permissible number of I/O modules exceeded.	- Switch off the power to the controller. - Reduce the number of I/O modules to an acceptable value. - Switch the power back on.
n*	Local bus disruption after the n^{th} process data module.	- Switch off the power to the controller. - Replace the $(n+1)^{th}$ process data module. - Switch the power back on. I/O modules that do not provide any data are ignored (e.g., supply module without diagnostics).

Table 53: Error Code 5, Explanation of Blink Codes and Procedures for Troubleshooting

Error Argument	Cause	Solution
n*	Register communication error during local bus initialization	- Switch off the power to the controller. - Replace the $(n+1)^{th}$ process data module. - Switch the power back on. I/O modules that do not provide any data are ignored (e.g., supply module without diagnostics).

Table 54: Error Code 7, Explanation of Blink Codes and Procedures for Troubleshooting

Error Argument	Cause	Solution
n	First unsupported I/O module in place of n.	- Switch off the power to the controller. - Replace the nth I/O module containing process data or reduce the number of modules to the number of n-1. - Switch the power back on.

Table 55: Error Code 9, Explanation of Blink Codes and Procedures for Troubleshooting

Error Argument	Cause	Remedy
1	Invalid program statement	Malfunction of the program sequence: - Contact WAGO Support.
2	Stack overflow	Malfunction of the program sequence: - Contact WAGO Support.
3	Stack underflow	Malfunction of the program sequence: - Contact WAGO Support.
4	Invalid event (NMI)	Malfunction of the program sequence: - Contact WAGO Support.
5	Local bus watchdog has triggered.	For ***e!****RUNTIME* applications: - Check the system load by IEC tasks with priorities 1 ... 14 in the runtime system (see Section “***e!****RUNTIME*” Runtime Environment > “CODESYS V3 Priorities”). For C applications: - Check the time monitoring settings.

11.2.4 Meaning of Blink Codes and Procedures for Troubleshooting

This section describes the diagnostics presented as blink codes via the MS LEDs.

If the diagnostics cannot be cleared by the measured specified for them, contact WAGO support. Be ready to explain to them the blink code that is displayed.

Phone: +49 571 887 44 55 5
Fax: +49 571 887 84 45 55
E-mail: support@wago.com

Table 56: Overview of MS-LED Error Codes

Error Code	Explanation
1	Configuration error

Table 57: Error Code 1, Explanation of Blink Codes and Procedures for Troubleshooting

Error Argument	Cause	Remedy
5	Error when synchronizing the controller configuration with the local bus	- Check the information of the connected I/O modules in the CODESYS controller configuration. - Adjust this to match the I/O module that is actually inserted. - Recompile the project. - Reload the project into the controller.

12 Service

12.1 Inserting and Removing the Memory Card

12.1.1 Inserting the Memory Card

1. Use an actuating tool or a screwdriver to open the transparent cover flap by flipping it upwards. The point where to position the tool is marked with an arrow.
2. Hold the memory card so that the contacts are visible on the right and the diagonal edge is at the top, as depicted in the figure below.
3. Insert the memory card in this position into the slot provided for it.
4. Push the memory card all the way in. When you let go, the memory card will move back a little and then snap in place (push-push mechanism).
5. Close the cover flap by flipping it down and pushing it in until it snaps into place.
6. You can seal the closed flap through the hole in the enclosure next to the flap.

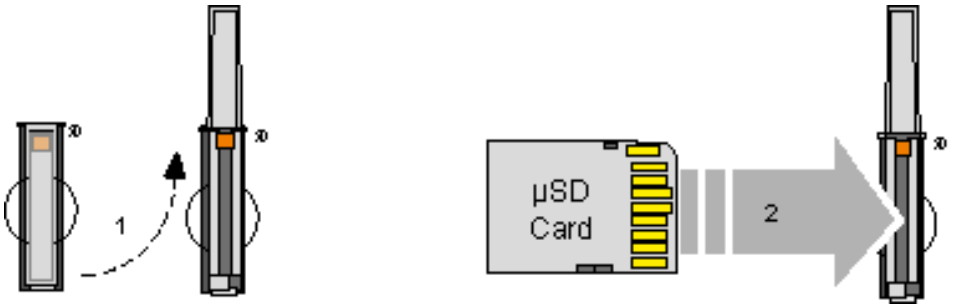


Figure 52: Inserting the Memory Card

12.1.2 Removing the Memory Card

1. First, remove any seal that may be in place.
2. Use an actuating tool or a screwdriver to open the transparent cover flap by flipping it upwards. The point where to position the tool is marked with an arrow.
3. To remove the memory card you must first push it slightly into the slot (push-push mechanism). This releases the mechanical locking mechanism.
4. As soon as you let go of the memory card, the memory card is pushed out a bit and you can remove it.
5. Remove the memory card.

6. Close the cover flap by flipping it down and pushing it in until it snaps into place.

12.2 Firmware Changes

NOTICE

Do not switch the controller off!
The controller can be damaged by interrupting the factory reset process.
Do not switch the controller off during the factory reset process, and do not disconnect the power supply!

Note

Obtain documentation appropriate for the firmware target version!
A firmware change can modify, remove or add controller properties and functions. As a result, described properties or functions of the controller may not be available or available properties or functions may not be described in the documentation.

Therefore, use only documentation appropriate for the target firmware after a firmware change.

If you have any questions, feel free to contact our WAGO Support.

Note

Note the firmware version
For devices with a factory installation of a firmware >= FW 05, a simple downgrade to a version <= FW 04 is not possible!
Use a special downgrade image.

You can update the firmware in two different ways using:

- ***e!****COCKPIT*
- WAGOupload
- Memory card and WBM

12.2.1 Use *e!COCKPIT* to Update/Downgrade the Firmware

1. Launch ***e!****COCKPIT*.
2. Create a new project or open an existing project.
3. Add at least one controller to your ***e!****COCKPIT* project either by scanning the network or going to the device catalog and entering the IP address of your controller in the settings dialog.

   Your controller is now displayed in the Device View of the project.
4. Select the displayed controller and click “Apply Selection” in the “SCAN” tab.
5. Click **[Add]** in the dialog.
6. Then click **[Replace Firmware]**. in the “DEVICE” tab.

   The “Replace Firmware” dialog opens.
7. In the “Replace Firmware” dialog, select the required firmware under “Available firmware on the PC” or click the “Select File” entry and select the * .wup firmware file for the required firmware.
8. Click **[Replace Firmware]** to transfer the firmware to the controller.
9. Wait until the operation ends with a status message and only then click **[OK]** to close the window.

The newly installed firmware is now available on your controller.

12.2.2 Use WAGOupload to Update/Downgrade the Firmware

1. Launch WAGOupload.
2. Click the **[Update Firmware]** action.
3. In the “Select Target Controllers” dialog, enter the IP address of your controller in the “Transfer via TCP/IP” option.
4. Click **[Find Controller]**.

   Your controller is now displayed in the list.
5. Select the displayed controller and click **[Next]**.
6. In the “Select Update File” dialog, select the *.wup firmware file for the required firmware.
7. Click **[Next]**.
8. Click **[Next]** to confirm the summary.
9. Wait until the operation ends with a status message and only then click **[Exit]** to close the window.

The newly installed firmware is now available on your controller.

12.2.3 Perform Firmware Update/Downgrade

Proceed as follows if you want to update the controller to a later firmware version or to downgrade the controller to an earlier firmware version:

1. Copy the firmware image (*.img file) of the required firmware to the memory card using a suitable PC tool.
2. Save your application and the controller settings.
3. Switch off the controller.
4. Insert the memory card with the new firmware image into the memory card slot. Use a special downgrade image if necessary (see above).
5. Switch on the controller.
6. After booting the controller, launch the WBM “Create Boot Image” page (you may have to temporarily change the IP address).
7. Create a new boot image on the internal memory.
8. Switch off the controller after completing the process.
9. Remove the memory card.
10. Switch on the controller.

The controller can now be started with the new firmware version.

12.3 Updating Root Certificates

If you want to update the root certificates on the controller, proceed as follows:

1. Download the current root CA bundle from https://curl.haxx.se/ca to your PC.
2. Rename the file “ca-certificates.crt.”
3. Transfer the file to the /etc/ssl/certs directory on the controller with an SFTP or FTP client.
4. Restart the controller. To do so, use the reboot function in WBM or CBM.

13 Removal

⚠ CAUTION

Risk of injury due to sharp-edged blade contacts!
The blade contacts are sharp-edged. Handle the I/O module carefully to prevent injury. Do not touch the blade contacts.

13.1 Removing Devices

⚠ DANGER



Do not work when devices are energized!
High voltage can cause electric shock or burns.
Switch off all power to the device prior to performing any installation, repair or maintenance work.

13.1.1 Removing the Controller

1. Use a screwdriver blade to turn the locking disc until the nose of the locking disc no longer engages behind the carrier rail.

2. Remove the controller from the assembly by pulling the release tab.

Electrical connections for data or power contacts to adjacent I/O modules are disconnected when removing the controller.

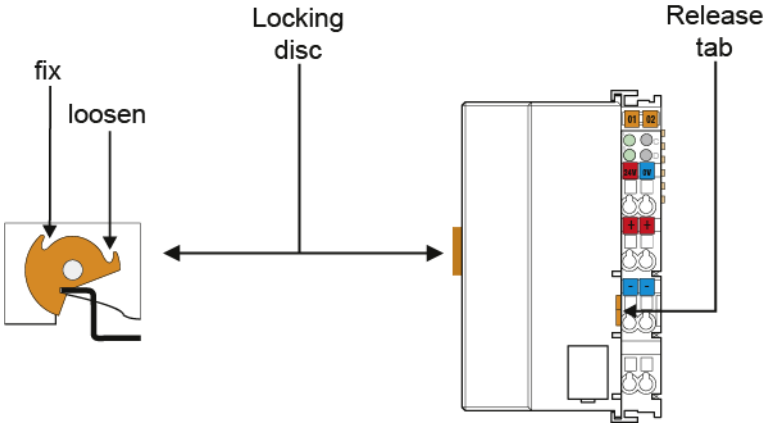


Figure 53: Release Tab of Controller

14 Disposal

14.1 Electrical and electronic equipment



Electrical and electronic equipment may not be disposed of with household waste. This also applies to products without this symbol.

Electrical and electronic equipment contain materials and substances that can be harmful to the environment and health. Electrical and electronic equipment must be disposed of properly after use.
WEEE 2012/19/EU applies throughout Europe. Directives and laws may vary nationally.



Environmentally friendly disposal benefits health and protects the environment from harmful substances in electrical and electronic equipment.

- Observe national and local regulations for the disposal of electrical and electronic equipment.
- Clear any data stored on the electrical and electronic equipment.
- Remove any added battery or memory card in the electrical and electronic equipment.
- Have the electrical and electronic equipment sent to your local collection point.

Improper disposal of electrical and electronic equipment can be harmful to the environment and human health.

14.2 Packaging

Packaging contains materials that can be reused.
PPWD 94/62/EU and 2004/12/EU packaging guidelines apply throughout Europe. Directives and laws may vary nationally.

Environmentally friendly disposal of the packaging protects the environment and allows sustainable and efficient use of resources.

- Observe national and local regulations for the disposal of packaging.

- Dispose of packaging of all types that allows a high level of recovery, reuse and recycling.

Improper disposal of packaging can be harmful to the environment and wastes valuable resources.

15 Use in Hazardous Environments

The **WAGO I/O System 750** (electrical equipment) is designed for use in Zone 2 hazardous areas and shall be used in accordance with the marking and installation regulations.

The following sections include both the general identification of components (devices) and the installation regulations to be observed. The individual subsections of the “Installation Regulations” section must be taken into account if the I/O module has the required approval or is subject to the range of application of the ATEX directive.

15.1 Marking Configuration Examples

15.1.1 Marking for Europe According to ATEX and IECEx

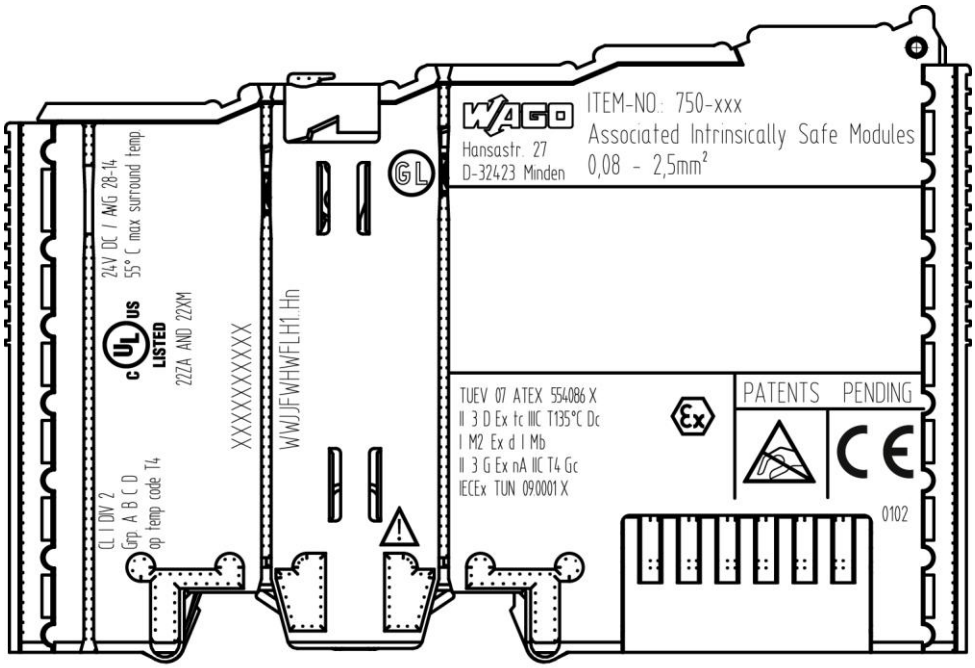


Figure 54: Marking Example According to ATEX and IECEx

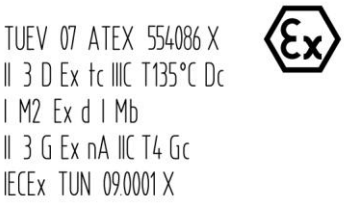


Figure 55: Text Detail – Marking Example According to ATEX and IECEx

Table 58: Description of Marking Example According to ATEX and IECEx

Marking	Description
TUEV 07 ATEX 554086 X IECEx TUN 09.0001 X	Approving authority resp. certificate numbers
Dust	
II	Equipment group: All except mining
3 D	Category 3 (Zone 22)
Ex	Explosion protection mark
tc	Type of protection: Protection by enclosure
IIIC	Explosion group of dust
T135°C	Max. surface temperature of the enclosure (without a dust layer)
Dc	Equipment protection level (EPL)
Mining	
I	Equipment group: Mining
M2	Category: High level of protection
Ex	Explosion protection mark
d	Type of protection: Flameproof enclosure
I	Explosion group for electrical equipment for mines susceptible to firedamp
Mb	Equipment protection level (EPL)
Gases	
II	Equipment group: All except mining
3 G	Category 3 (Zone 2)
Ex	Explosion protection mark
nA	Type of protection: Non-sparking equipment
IIC	Explosion group of gas and vapours
T4	Temperature class: Max. surface temperature 135 °C
Gc	Equipment protection level (EPL)

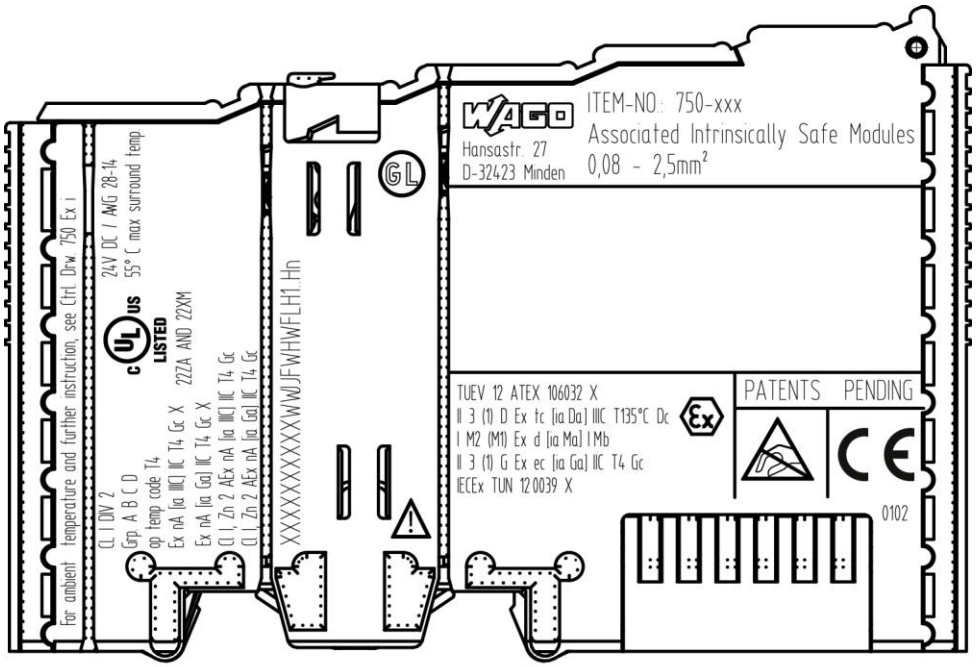


Figure 56: Marking Example for Approved I/O Module Ex i According to ATEX and IECEx



Figure 57: Text Detail – Marking Example for Approved I/O ModuleEx i According to ATEX and IECEx

Table 59: Description of Marking Example for Approved I/O Module Ex I According to ATEX and IECEx

Marking	Description
TUEV 12 ATEX 106032 X IECEx TUN 12 0039 X	Approving authority resp. certificate numbers
Dust	
II	Equipment group: All except mining
3 (1) D	Category 3 (Zone 22) equipment containing a safety device for a category 1 (Zone 20) equipment
Ex	Explosion protection mark
tc	Type of protection: Protection by enclosure
[ia Da]	Type of protection and equipment protection level (EPL): Associated apparatus with intrinsic safety circuits for use in Zone 20
IIIC	Explosion group of dust
T135°C	Max. surface temperature of the enclosure (without a dust layer)
Dc	Equipment protection level (EPL)
Mining	
I	Equipment Group: Mining
M2 (M1)	Category: High level of protection with electrical circuits which present a very high level of protection
Ex	Explosion protection mark
d	Type of protection: Flameproof enclosure
[ia Ma]	Type of protection and equipment protection level (EPL): Associated apparatus with intrinsic safety electrical circuits
I	Explosion group for electrical equipment for mines susceptible to firedamp
Mb	Equipment protection level (EPL)
Gases	
II	Equipment group: All except mining
3 (1) G	Category 3 (Zone 2) equipment containing a safety device for a category 1 (Zone 0) equipment
Ex	Explosion protection mark
ec	Equipment protection by increased safety “e”
[ia Ga]	Type of protection and equipment protection level (EPL): Associated apparatus with intrinsic safety circuits for use in Zone 0
IIC	Explosion group of gas and vapours
T4	Temperature class: Max. surface temperature 135 °C
Gc	Equipment protection level (EPL)

15.1.2 Marking for the United States of America (NEC) and Canada (CEC)

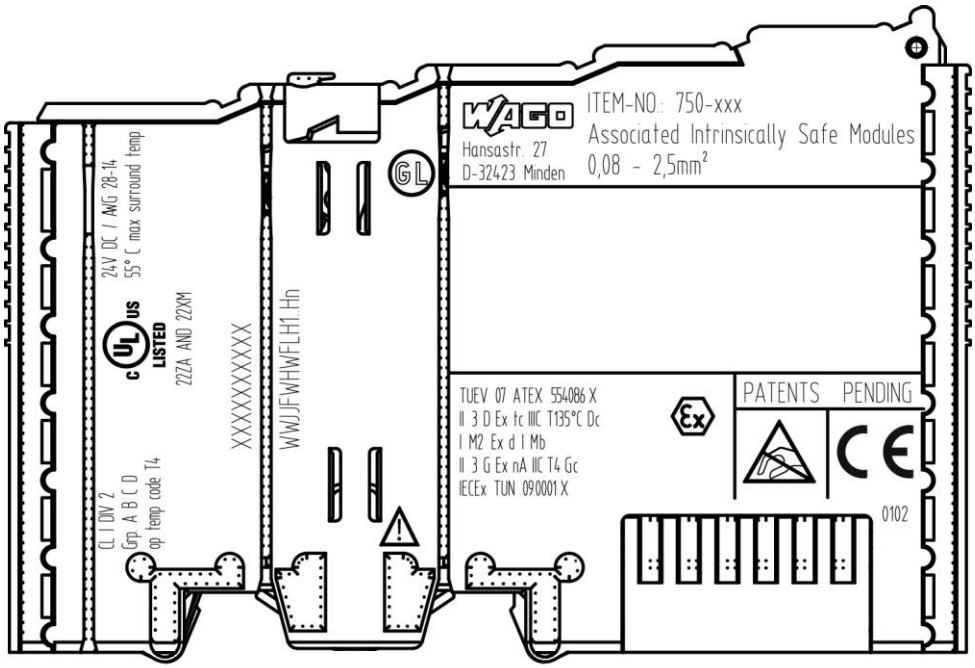


Figure 58: Marking Example According to NEC

CL I DIV 2
Grp. A B C D
op temp code T4

Figure 59: Text Detail – Marking Example According to NEC 500

Table 60: Description of Marking Example According to NEC 500

Marking	Description
CL I	Explosion protection (gas group)
DIV 2	Area of application
Grp. A B C D	Explosion group (gas group)
op temp code T4	Temperature class



Figure 60: Text Detail – Marking Example for Approved I/O Module Ex i According to NEC 505

Table 61: Description of Marking Example for Approved I/O Module Ex i According to NEC 505

Marking	Description
Cl I,	Explosion protection group
Zn 2	Area of application
AEx	Explosion protection mark
nA	Type of protection
[ia Ga]	Type of protection and equipment protection level (EPL): Associated apparatus with intrinsic safety circuits for use in Zone 20
IIC	Group
T4	Temperature class
Gc	Equipment protection level (EPL)



Figure 61: Text Detail – Marking Example for Approved I/O Module Ex i According to NEC 506

Table 62: Description of Marking Example for Approved I/O Module Ex i According to NEC 506

Marking	Description
Cl I,	Explosion protection group
Zn 2	Area of application
AEx	Explosion protection mark
nA	Type of protection
[ia IIIC]	Type of protection and equipment protection level (EPL): Associated apparatus with intrinsic safety circuits for use in Zone 20
IIC	Group
T4	Temperature class
Gc	Equipment protection level (EPL)



Figure 62: Text Detail – Marking Example for Approved I/O Module Ex i According to CEC 18 attachment J

Table 63: Description of Marking Example for Approved I/O Module Ex i According to CEC 18 attachment J

Marking	Description
Dust	
Ex	Explosion protection mark
nA	Type of protection
[ia IIIC]	Type of protection and equipment protection level (EPL): Associated apparatus with intrinsic safety circuits for use in Zone 20
IIC	Group
T4	Temperature class
Gc	Equipment protection level (EPL)
X	Symbol used to denote specific conditions of use
Gases	
Ex	Explosion protection mark
nA	Type of protection
[ia Ga]	Type of protection and equipment protection level (EPL): Associated apparatus with intrinsic safety circuits for use in Zone 0
IIC	Group
T4	Temperature class
Gc	Equipment protection level (EPL)
X	Symbol used to denote specific conditions of use

15.2 Installation Regulations

For the installation and operation of electrical equipment in hazardous areas, the valid national and international rules and regulations which are applicable at the installation location must be carefully followed.

15.2.1 Special Notes including Explosion Protection

The following warning notices are to be posted in the immediately proximity of the WAGO I/O System 750 (hereinafter “product”):

WARNING – DO NOT REMOVE OR REPLACE FUSED WHILE ENERGIZED!

WARNING – DO NOT DISCONNECT WHILE ENERGIZED!

WARNING – ONLY DISCONNECT IN A NON-HAZARDOUS AREA!

Before using the components, check whether the intended application is permitted in accordance with the respective printing. Pay attention to any changes to the printing when replacing components.

The product is an open system. As such, the product must only be installed in appropriate enclosures or electrical operation rooms to which the following applies:

- Can only be opened using a tool or key
- Inside pollution degree 1 or 2
- In operation, internal air temperature within the range of 0 °C ≤ Ta ≤ +55 °C or −20 °C ≤ Ta ≤ +60 °C for components with extension number …/025-xxx or −40 °C ≤ Ta ≤ +70 °C for components with extension number …/040-xxx
- Minimum degree of protection: min. IP54 (acc. to EN/IEC 60529)
- For use in Zone 2 (Gc), compliance with the applicable requirements of the standards EN/IEC/ABNT NBR IEC 60079-0, -7, -11, -15
- For use in Zone 22 (Dc), compliance with the applicable requirements of the standards EN/IEC/ABNT NBR IEC 60079-0, -7, -11, -15 and -31
- For use in mining (Mb), minimum degree of protection IP64 (acc. EN/IEC 60529) and adequate protection acc. EN/IEC/ABNT NBR IEC 60079-0 and -1
- Depending on zoning and device category, correct installation and compliance with requirements must be assessed and certified by a “Notified Body” (ExNB) if necessary!

Explosive atmosphere occurring simultaneously with assembly, installation or repair work must be ruled out. Among other things, these include the following activities

- Insertion and removal of components
- Connecting or disconnecting from fieldbus, antenna, D-Sub, ETHERNET or USB connections, DVI ports, memory cards, configuration and programming interfaces in general and service interface in particular:
  - Operating DIP switches, coding switches or potentiometers
  - Replacing fuses

Wiring (connecting or disconnecting) of non-intrinsically safe circuits is only permitted in the following cases

- The circuit is disconnected from the power supply.
- The area is known to be non-hazardous.

Outside the device, suitable measures must be taken so that the rated voltage is not exceeded by more than 40 % due to transient faults (e.g., when powering the field supply).

Product components intended for intrinsically safe applications may only be powered by 750-606 or 750-625/000-001 bus supply modules.

Only field devices whose power supply corresponds to overvoltage category I or II may be connected to these components.

15.2.2 Special Notes Regarding ANSI/ISA Ex

For ANSI/ISA Ex acc. to UL File E198726, the following additional requirements apply:

- Use in Class I, Division 2, Group A, B, C, D or non-hazardous areas only
- ETHERNET connections are used exclusively for connecting to computer networks (LANs) and may not be connected to telephone networks or telecommunication cables
- **WARNING** – The radio receiver module 750-642 may only be used to connect to external antenna 758-910!
- **WARNING** – Product components with fuses must not be fitted into circuits subject to overloads!
  These include, e.g., motor circuits.
- **WARNING** – When installing I/O module 750-538, “Control Drawing No. 750538” in the manual must be strictly observed!



Information

Additional Information
Proof of certification is available on request.
Also take note of the information given on the operating and assembly instructions.
The manual, containing these special conditions for safe use, must be readily available to the user.

16 Appendix

16.1 Configuration Dialogs

16.1.1 Web-Based-Management (WBM)

16.1.1.1 “Information” Tab

16.1.1.1.1 “Device Status” Page

The “Device Status” page shows information about product identification and the most important network properties.

“Device Details” Group

This group shows information about product identification.

Table 64: WBM “Device Status” Page – “Device Details” Group

Parameters	Explanation
Product Description	Product Designation
Order Number	Product Item Number
Serial	Unique Product Serial Number
License Information	Notification that the CODESYS runtime system is available
Firmware Revision	Firmware Version

“Network TCP/IP Details” Group

The network and interface properties of the product are displayed in this group.

Table 65: WBM “Device Status” Page – “Network TCP/IP Details” Group

Parameter	Meaning	
DIP Switch Status	Status of the address selection switch; this area only appears if an address selection switch is available.	
DIP Switch Mode	Address Selection Switch	
	Off (0)	IP address assignment via e.g., WBM
	static (1 … 254)	Static IP address assignment via address selection switch
	dhcp (255)	Dynamic IP address assignment via DHCP
DIP Switch Value	Set value of the address selection switch	
Bridge <n>	Bridge currently configured; the properties are displayed in a separate area for each configured bridge.	
MAC Address	MAC address used for product identification and addressing	
IP Source	Current reference type of the IP address	
	none	No IP allocation method is selected; this occurs, for example, if a bridge was added due to changes to the bridge configuration. Select a source in the **Configuration** tab on the **Networking** > **TCP/IP Configuration** page.
	static IP	Static IP address assignment
	dhcp	Dynamic IP address assignment via DHCP
	bootp	Dynamic IP address assignment via BootP (if BootP is supported)
	external	The IP address may be assigned by the fieldbus application; this occurs e.g., if the IP address is controlled by the application.
IP Address	Current product IP address	
Subnet Mask	Current product subnet mask	

16.1.1.1.2 “Vendor Information” Page

You can find the manufacturer and address on the “Vendor Information” page.

16.1.1.1.3 “PLC Runtime Information” Page

All information about the enabled runtime system and PLC program created in the programming software is provided on the “PLC Runtime Information” page. You will also find a link here to open WebVisu.

“Runtime” Group

Table 66: WBM “PLC Runtime Information” Page – “Runtime” Group

Parameter	Explanation	
Version	The version of the currently enabled runtime system is shown. If the runtime system is disabled, “None” is displayed and the subsequent fields of this group are hidden.	
Webserver Version	This shows the version number of the Webserver. This field appears if the controller supports the CODESYS V2 runtime system and CODESYS V2 is set as the runtime system.	
State	The PLC operating state is displayed. This field appears if the controller supports the CODESYS V2 runtime system and CODESYS V2 is set as the runtime system.	
	STOP	PLC program is not executed.
	RUN	PLC program is executed.
Number of Tasks	The number of tasks in the PLC program is shown. This field appears if the controller supports the CODESYS V2 runtime system and CODESYS V2 is set as the runtime system.	

“WebVisu” Group

You will find a link that you can use to open WebVisu.

“Project Details” Group

This group appears if the controller supports the CODESYS V2 runtime system and CODESYS V2 is set as the runtime system.

Table 67: WBM “PLC Runtime Information” Page – “Project Details” Group

Parameter	Explanation
Date	The last save date of the project is displayed.
Title	The project information that the programmer has entered in the PLC program is displayed here (in the programming software under Project > Project Information ...). The information only appears in an executed PLC program. Descriptive texts up to 1024 characters long are given under “Description.”
Version	
Author	
Description	
Checksum	The calculated checksum of the project is displayed.

“Task <n>” Group(s)

One dedicated group is displayed for each task when the PLC program is executed. As a rule, only the group title is displayed with the task number, the task name and the task ID.

This group(s) appear(s) if the controller supports the CODESYS V2 runtime system and CODESYS V2 is set as the runtime system.

Table 68: WBM “PLC Runtime Information” Page – “Task n” Group(s)

Parameter	Explanation
Cycle count	Number of task cycles since the system start
Cycle time (µsec)	Currently measured task cycle time for the task
Cycle time min (µsec)	Minimum task cycle time for the task since the system start
Cycle time max (µsec)	Maximum task cycle time for the task since the system start
Cycle time avg (µsec)	Average task cycle time since the system start
Status	Task status (e.g., RUN, STOP)
Mode	Task execution mode (e.g., in cycles)
Priority	Set task priority
Interval (msec)	Set task interval

16.1.1.1.4 “WAGO Software License Agreement” Page

The “WAGO Software License Agreement” page lists the license terms for the WAGO software used in the product.

16.1.1.1.5 “Open Source Licenses” Page

The license conditions for the open source software used for the product are listed in alphabetical order on the “Open Source Licenses” page.

16.1.1.1.6 “WBM Third Party License Information” Page

On the “WBM Third Party License Information” page, you can find the license text of the open source licenses that apply to the WBM itself.

16.1.1.1.7 “Trademarks Information” Page

On the “Trademarks Information” page you will find a list of property and trademark rights.

16.1.1.1.8 “WBM Version” Page

On the “WBM Version” page, you can find the version information for the various sections (“Plug-ins”) that the WBM contains. This information may be useful for support if an error is found in the WBM.

16.1.1.2 “Configuration” Tab

16.1.1.2.1 “PLC Runtime Configuration” Page

On the "PLC Runtime Configuration" page, you will find the settings for the boot project created with the programming software and the settings for the web visualization created in the runtime system.

“General PLC Runtime Configuration” Group

Table 69: WBM “PLC Runtime Configuration” Page – “General PLC Runtime Configuration” Group

Parameter	Meaning	
PLC runtime version	Select here the PLC runtime system to be enabled.	
	None	No runtime system is enabled.
	CODESYS 2	CODESYS V2 runtime system is enabled. This value only appears if the controller supports the CODESYS V2 runtime system.
	e!*RUNTIME*	***e!****RUNTIME* runtime system is enabled. This value only appears if the controller supports the ***e!****RUNTIME* runtime system.
Home directory on memory card enabled	Define if the home directory for the runtime system should be moved to the memory card.	
	Disabled	The home directory is stored in the internal memory.
	Enabled	The home directory is moved to the memory card.

Note

All data is deleted when switching the runtime system!
The runtime system’s home directory is completely deleted when switching the runtime system!

Note

Only the first partition can be used as the Home directory!
Only the first partition of a memory card can be accessed at **/media/sd** and used as the home directory.

Click **[Submit]** to apply the change. The runtime system change is effective immediately.
The home directory change only takes effect after the product restarts. For this purpose, use the WBM reboot function. Do not switch off the product too early!

“Webserver Configuration” Group

Table 70: WBM “PLC Runtime Configuration” Page – “Webserver Configuration” Group

Parameter	Meaning	
CODESYS V2 Webserver State	This displays the status (enabled/disabled) of the CODESYS V2 Webserver. This field only appears if the controller supports the CODESYS V2 runtime system.	
e!*RUNTIME* Webserver State	This indicates the status (enabled/disabled) of the ***e!****RUNTIME* Webserver. This field only appears if the controller supports the ***e!****RUNTIME* runtime system.	
Default Webserver	Choose here whether the Web-based Management or web visualization of the runtime system should be displayed when only entering the IP address of the controller.	
	Web-Based Management	The Web-based Management is displayed.
	WebVisu	The web visualization of the runtime system is displayed.

Click **[Submit]** to apply the change. The change takes effect immediately.

In its default setting, the WBM is called up when only entering the IP address.

To update the display after switching, enter the IP address again in the address line of the Web browser.

To display the web visualization, the Webserver must be enabled (in WBM under “Ports and Services” -> “PLC Runtime Services”) and there must be a suitably configured application.

Regardless of the default Webserver setting, the WBM can be called up at any time with “https://<IP address>/wbm” and the Web visualization with “https://<IP address>/webvisu”.



Note

Possible error messages when calling up the web visualization
The “500 − Internal Server Error” message indicates that the Webserver is not enabled.
A page with the header “WebVisu not available” means that no application has been loaded in the product using web visualization.

16.1.1.2.2 “TCP/IP Configuration” Page

The TCP/IP settings for the ETHERNET interfaces are shown on the “TCP/IP configuration” page.

“TCP/IP Configuration” Group

The properties are displayed in a separate area for each configured bridge.

Table 71: WBM “TCP/IP Configuration” Page – “TCP/IP Configuration” Group

Parameter	Meaning	
Network Details Bridge <n>	Settings for the bridge currently configured	
Current IP Address	This displays the current IP address.	
Current Subnet Mask	This displays current subnet mask.	
Current Default Gateway	The IP address of the current default gateway is displayed.	
IP Source	You can specify whether to use a static or dynamic IP address.	
	Static IP	Static IP addressing
	DHCP	Dynamic IP addressing via DHCP
	BootP	Dynamic IP addressing via BootP
IP Address	Enter a static IP address. This is enabled if “Static IP” is enabled in the **IP Source** field.	
Subnet Mask	Enter the subnet mask. This is enabled if “Static IP” is enabled in the **IP Source** field.	
Default Gateway	Enter the IP address of the default gateway here.	

Click the **[Submit]** button to apply a change. The change takes effect immediately.

“DNS Server” Group

Table 72: WBM “TCP/IP Configuration” Page – “DNS Server” Group

Parameters	Explanation
Active	The active DNS servers are displayed. Up to 3 active DNS servers can be used. The index reflects the query order. The first DNS server assigned via DHCP is given the highest priority.
Assigned by DHCP	The DNS servers assigned if necessary by DHCP (or BootP) are displayed. If no DNS server has been assigned by DHCP (or BootP), “No DNS Servers assigned by DHCP” is displayed.
Assigned by user	The addresses of the defined DNS servers are displayed. If no server has been entered, “No DNS Servers configured” is displayed.
New Server IP	Add additional DNS server addresses. You can enter as many addresses as you like, but a maximum of three entries are used. The entries actually used result from an alternating combination of the “Assigned by DHCP” and ”Assigned by user” lists.

Click the **[Delete]** button to delete the selected DNS server. The change takes effect immediately.

Click the **[Add]** button to add the entered DNS server. The change takes effect immediately.

16.1.1.2.3 “Ethernet Configuration” Page

The settings for ETHERNET are located on the “Ethernet Configuration” page.

“Bridge Configuration” Group

Table 73: WBM “Ethernet Configuration” Page – “Bridge Configuration” Group

Parameter	Meaning
Bridge 1 … <n>	Assign the physical ports X1… X <n> to a logical bridge. To do so, click the respective option button. The assignment is marked in color. A port can only be assigned to one bridge at a time.

Click the **[Submit]** button to apply the change. The change takes effect immediately.

“Switch Configuration” Group

This group only appears if parameter configuration is supported.

Table 74: WBM “Ethernet Configuration” Page – “Switch Configuration” Group

Parameters	Explanation	
Port Mirror	Enable or disable mirroring of the data traffic between the ports.	
	None	Both ETHERNET ports are operating normally.
	X1	The entire data traffic between X1 and the PFC system is mirrored at port X2.
	X2	The entire data traffic between X2 and the PFC system is mirrored at port X1.
Broadcast Protection	You can set the broadcast limit for protection against overloads.	
	Disabled	No broadcast packet limit
	1 % … 5 %	Limits incoming broadcast packets to the selected percentage of the total possible data throughput (10/100 Mbit)
Rate Limit	You can set the basic limitation of the incoming data traffic.	
	Disabled	No limitation of the incoming data traffic
	64 kbps … 99 mbps	Limits the incoming data traffic to the entered value

Click **[Submit]** to apply the change. The change takes effect immediately.

“Ethernet Interface Configuration” Group

Table 75: WBM “Ethernet Configuration” Page – “Ethernet Interface Configuration” Group

Parameter	Meaning
Interface X<n>	A separate area is displayed for each interface in the controller.
Enabled	You can enable or disable the interface.
MAC Learning	You can disable or enable “MAC Learning”.
Speed/Duplex	Select the transmission speed and the transmission method. The drop-down menu is generated depending on the device and interface. When “Autonegotiation” is selected, the connection modalities are negotiated automatically between the peer devices.

Click **[Submit]** to apply changes. The changes take effect immediately.

16.1.1.2.4 Configuration of Host and Domain Name" Page

The settings for the hostname and domain are displayed on the "Configuration of Host/Domain Name" page.

"Hostname" Group

Table 76: WBM "Configuration of Host and Domain Name" Page – "Hostname" Group

Parameter	Explanation
Currently used	If you have selected dynamic assignment of an IP address via DHCP, the name of the host currently being used is displayed.
Configured	Enter the product hostname here; it is then used if the network interface is changed to a static IP address or if no hostname is assigned per DHCP response.

Click the **[Submit]** button to apply a change.

Click the **[Clear]** button to reset the input field.

The change takes effect immediately.

If the controller has been assigned a host name via DHCP, it is given preference and the manually configured host name is not used.
To accept the manually configured host name, the configuration of the DHCP server may have to be reduced by assigning the host name.

"Domain Name" Group

Table 77: WBM "Configuration of Host and Domain Name" Page – "Domain Name" Group

Parameter	Explanation
Currently used	If you have selected dynamic assignment of an IP address via DHCP, the name of the domain currently being used is displayed.
Configured	Enter the product domain name here; it is then used if the network interface is changed to a static IP address or if no domain name is assigned per DHCP response.

Click the **[Submit]** button to apply a change.

Click the **[Clear]** button to reset the input field.

The change takes effect immediately.

If the controller has been assigned a domain name via DHCP, it is given preference and the manually configured domain name is not used.
To accept the manually configured domain name, the configuration of the DHCP server may have to be reduced by assigning the domain name.

16.1.1.2.5 “Routing” Page

On the “Routing” page you can find settings and information on the routing between the network interfaces.

“IP Forwarding through multiple interfaces” Group

Table 78: WBM “Routing” Page – “IP Forwarding through multiple interfaces” Group

Parameter	Explanation
Enabled	Specify whether forwarding of IP data packets is allowed between different network interfaces. If the box is not checked, the settings under “Static Routes” are used, without allowing IP data packets that arrive at the controller on one network interface to leave the controller on different network interface. If the box is checked, IP packets can be forwarded between the interfaces. Other settings may be necessary on this WBM page.

Click the **[Submit]** button to apply the change. The changes take effect immediately.

“Custom Routes” Group

Each configured static route has its own area in the display. If no static routes have been entered, “(no custom routes)” is displayed.

Table 79: WBM “Routing” Page – “Custom Routes“ Group

Parameter	Explanation	
Enabled	Specify whether the selected route should be used.	
	Disabled	The route is not used.
	Enabled	The route is used.
Destination Address	Specify whether any network devices or only a specific network device or device pool should be accessible.	
	Default	Any network devices can be reached.
	Network address	Only a specific network device or device from the specified address pool can be reached.
Destination Mask	Enter the subnet mask of the device. If “default” is entered for Destination Address, the value “0.0.0.0” must be entered.	
Gateway Address	Enter the address of the gateway. If the “Interface” input field is empty, an entry is required here. If a value is entered in the “Interface” input field, the input here is optional.	
Gateway Metric	Set the number used as the metric. When there are multiple routes with the same destination address and destination mask, the metric specifies the gateway to which network data packets are first sent. Priority is given to routes with a lower value for the metric. The lowest value is 0. The highest value is $2^{32} - 1 = 4294967295$.	
Interface	Enter an interface via which the packets sent to the destination address are routed. Bridges (br0-br3) as well as modems (wwan0) or VPN interface names can be used. If the “Gateway Address” input field is empty, an entry is required here. If a value is entered in the “Gateway Address” input field, the input here is optional.	

Click the **[Submit]** button to apply the changes. The changes take effect immediately.

To add a new route, click the **[Add]** button. The change takes effect immediately.

Click the **[Delete]** button to delete an existing route. The change takes effect immediately.

“Dynamic Routes” Group

All default gateways received via DHCP are displayed.
Default gateways configured via DHCP are given the metric value 10, which means that they are normally used before the statically configured default gateways.

Each dynamic route has its own area in the display. If no dynamic routes are received via DHCP, “(no dynamic route)” appears.

“IP-Masquerading” Group

Each entry has its own area in the display.

Table 80: WBM “Routing” Page – “IP-Masquerading” Group

Parameters	Explanation	
Enabled	Specify whether IP masquerading should be used.	
	Disabled	IP masquerading is not used.
	Enabled	IP masquerading is used.
Interface	You can select the specified name of a network interface. Alternatively, selecting “other” allows you to specify any network interface name.	

Click the **[Submit]** button to apply the changes. The changes take effect immediately.

Click the **[Add]** button to add a new entry. The change takes effect immediately.

Click the **[Delete]** button to delete an existing entry. The change takes effect immediately.

An entry is only transferred to the system if “Enabled” is enabled in the “General Routing Configuration” group. This allows you to configure a default setting that is not applied until the general switch-on.

“Port-Forwarding” Group

Each entry has its own area in the display.

Table 81: WBM “Routing” Page – “Port Forwarding” Group

Parameters	Explanation	
Enabled	Specify whether port forwarding should be used.	
	Disabled	Port forwarding is not used.
	Enabled	Port forwarding is used.
Interface	You can select the specified name of a network interface. Alternatively, selecting “other” allows you to specify any network interface name.	
Port	Enter the port here on which the product receives network data packets to be forwarded.	
Protocol	You can select the protocol to be used for the port forwarding. The options are TCP, UDP or both protocols.	
Destination Address	Specify the network address of the destination device. This address replaces the original destination address of the network data packet.	
Destination Port	Specify the port number of the destination device. This value replaces the original destination port of the network data packet.	

Click the **[Submit]** button to apply the changes. The changes take effect immediately.

Click the **[Add]** button to add a new entry. The change takes effect immediately.

Click the **[Delete]** button to delete an existing entry. The change takes effect immediately.

An entry is only transferred to the system if “Enabled” is enabled in the “General Routing Configuration” group. This allows you to configure a default setting that is not applied until the general switch-on.

16.1.1.2.6 “Clock Settings” Page

The date and time settings are displayed on the “Clock Settings” page.

“Timezone and Format” Group

Table 82: WBM “Clock Settings” Page – “Timezone and Format” Group

Parameter	Explanation	
Timezone	Select the appropriate time zone for your location. Default setting:	
	AST/ADT	“Atlantic Standard Time,” Halifax
	EST/EDT	“Eastern Standard Time,” New York, Toronto
	CST/CDT	“Central Standard Time,” Chicago, Winnipeg
	MST/MDT	“Mountain Standard Time,” Denver, Edmonton
	PST/PDT	“Pacific Standard Time”, Los Angeles, Whitehouse
	GMT/BST	“Greenwich Mean Time”, GB, P, IRL, IS, …
	CET/CEST	“Central European Time,” B, DK, D, F, I, CRO, NL, …
	EET/EEST	“Eastern European Time,” BUL, FI, GR, TR, …
	CST	“China Standard Time”
	JST	“Japan/Korea Standard Time”
TZ string	For time zones that cannot be selected with the “Time Zone” parameter, enter the name of the time zone or the country or city applicable to you. You can determine a valid name for the time zone here: http://www.timeanddate.com/time/map/	
Time Format	For switching between 12-hour and 24-hour time display	

Click the **[Submit]** button to apply a change. The change takes effect immediately.

“UTC Time and Date” Group

Table 83: WBM “Clock Settings” Page – “UTC Time and Date” Group

Parameter	Explanation
UTC Date	Set the date.
UTC Time	Set GMT time.

Click the **[Submit]** button to apply a change. The change takes effect immediately.

“Local Time and Date” Group

Table 84: WBM “Clock Settings” Page – “Local Time and Date” Group

Parameter	Explanation
Local Date	Set the date.
Local Time	Set the local time.

Click the **[Submit]** button to apply a change. The change takes effect immediately.

16.1.1.2.7 “Configuration of Service Interface” Page

The settings for the service interface are shown on the “Configuration of the Service Interface” page.

“Service Interface assigned to” Group

The application that the service interface is currently assigned to is displayed.

“Assign Owner of Service Interface” Group

You can specify the application to which the service interface is assigned after the next controller reboot.

Table 85: WBM “Configuration of Service Interface” Page – “Assign Owner of Service Interface” Group

Parameters	Explanation
WAGO Service Communication	Specify that the service interface is used for the WAGO Service communication or runtime system communication.
Linux Console	Specify that the service interface is assigned to the Linux® console.
Unassigned (usage by applications, libraries, CODESYS)	Specify that the service interface is not to be assigned to any application and is available, so that the CODESYS program, for example, can access it via function blocks.

Click **[Submit]** to apply the change. The change only takes effect once the controller restarts. For this purpose, use the WBM reboot function. Do not shut down the controller too early!

16.1.1.2.8 “Create Bootable Image” Page

You can create a bootable image on the “Create Bootable Image” page.

“Create bootable image from boot device” Group

Once the destination has been determined and output, it is then checked and the results of this check are displayed below the settings:

Table 86: WBM “Create Bootable Image” Page – “Create bootable image from active partition” Group

Parameters	Meaning		
Boot Device	The medium from which the boot was made is displayed.		
Destination	Depending on which medium has been booted, the following destination is available for selection after boot-up for the image to be generated:		
	System was booted from		Target partition for “bootable image”
	Memory Card	→	Internal Flash
	Internal memory	→	Memory Card

- Free space on target device:
  If the available memory space is less than 5% a warning is displayed. You can still start the copy process despite the warning. If the available space is too low, a corresponding message is displayed and copying cannot be started.

- Device being used by CODESYS:
  If the device is being used by CODESYS, a warning is displayed. Although it is not recommended, you can still start the copying procedure despite this warning.

Click **[Start Copy]** to start the copying procedure. If the outcome of the test is positive, copying begins immediately. If errors have been detected, a corresponding message is displayed and copying is not started. If warnings have been issued, these are displayed again and you must then confirm that you still wish to continue.

16.1.1.2.9 “Firmware Backup” Page

You can find the controller data backup settings on the “Firmware Backup” page.

“Firmware Backup” Group

Table 87: WBM “Firmware Backup” Page – “Firmware Backup” Group

Parameter	Explanation	
Boot Device	The storage medium from which the device was booted is displayed here.	
Destination	Select the storage location for the backup here.	
	Memory Card	The data is written to the memory card. This selection only appears if a memory card is inserted and the device has not been booted from the memory card.
	Network	The data is saved in the file system and then made available as a download on the PC.
PLC runtime project	If you want to save the PLC runtime project, select this checkbox.	
Settings	If you want to save the device settings, select this checkbox.	
System	If you want to back up the operating system of the device and the root file system, select this checkbox.	
Encryption	If you want to save the data in encrypted form, select this button.	
Encryption passphrase	Enter the encryption password here. This input field only appears if the “Encryption” checkbox is selected.	
Confirm passphrase	Enter the encryption password again here to check it. This input field only appears if the “Encryption” checkbox is selected.	

Note

Note the firmware version!
Restoring the controller operating system (“System” selection) is only permissible and possible if the firmware versions at the backup and restore times are identical.
If necessary, skip restoring the controller operating system, or match the firmware version of the controller to the firmware version of the backup time beforehand.

Note

Only one package may be copied to the network!
If you have specified “Network” as the storage location, only one package may be selected for each storing process.

Note

No backup of the memory card!
Backup from the memory card to the internal flash memory is not possible.

Note

Account for backup time!
Generation of backup files can take several minutes. Stop the CODESYS program before you start the backup procedure to help shorten the time required.

Click the **[Create Backup]** button to start the backup operation.

16.1.1.2.10 “Firmware Restore” Page

The settings for restoring the controller data are shown on the “Firmware Restore” page.

“Firmware Restore” Group

Table 88: WBM “Firmware Restore” Page – “Firmware Restore” Group

Parameter	Explanation	
Source	Select the data source for the restore here.	
	Memory Card	The data is read from the memory card. This selection is only enabled if a memory card is inserted and the device has not been booted from the memory card.
	Network	The data is uploaded from the PC and restored.
Boot Device	The storage medium from which the device was booted is displayed here.	
PLC runtime project	Enter the name of the backup file for the CODESYS project here. The input field only appears if the network is selected as the data source.	
Settings	Enter the name of the backup file for the settings here. The input field only appears if the network is selected as the data source.	
System	Enter the name of the backup file for the system data and the root file system here. The input field only appears if the network is selected as the data source.	
Decryption	If you have backed up the data in encrypted form, select this checkbox.	
Decryption passphrase	Enter the encryption password here. This input field only appears if the “Decryption” checkbox is selected.	



Note

Note the firmware version!

Restoring the controller operating system (“System” selection) is only permissible and possible if the firmware versions at the backup and restore times are identical.

If necessary, skip restoring the controller operating system, or match the firmware version of the controller to the firmware version of the backup time beforehand.

Note

File size must not exceed the size of the internal drive!
Note that the amount of data in the media/sd/copy/ directory must not exceed the total size of the internal drive.

Note

Restoration only possible from internal memory!
If the device was booted from the memory card, the firmware cannot be restored.

Note

Reset by restore
A reset is performed when the system or settings are restored by CODESYS!

Note

Connection loss through restore
If the restore changes the parameters of the ETHERNET connection, the WBM may then no longer be able to open a connection to the device. You must call the WBM again by entering the correct IP address of the device in the address line.

Note

Note the restore time!
The restore process takes approx. 2 … 3 minutes.
After the restore process, the controller is restarted and is then ready for use again.

Click the **[Restore]** button to start the restore operation.

16.1.1.2.11 “Active System” Page

The settings for specifying the partition from which the system is started are shown on the “Active System” page.

“Boot Device” Group

Table 89: WBM “Active System” Page – “Boot Device” Group

Parameter	Explanation
Boot Device	The storage medium from which the device was booted is displayed here.

“System <n> (Internal Flash)” Groups

Table 90: WBM “Active System” Page – “System <n> (Internal Flash)” Group

Parameter	Explanation	
Active	This shows whether the system is active.	
Configured	This shows whether the system should be active after the next reboot.	
State	The system status is displayed here.	
	good	The system is valid and can be used.
	bad	The system is not valid and cannot be used.

Click the respective **[Activate]** button to start the required system at the next reboot.



Note

Provide a bootable system!
A functional firmware backup must be available on the boot system!

16.1.1.2.12 “Mass Storage” Page

The “Mass Storage” page displays information and settings for the storage media.

The group title contains the designation for the storage media (“Memory Card” or “Internal Flash”) and, if this storage medium is also the active partition, the text “Active Partition”.

“Devices” Group

An area with information on the storage medium is displayed for each storage medium found.

Table 91: WBM “Mass Storage” Page – “Devices” Group

Parameter	Explanation
<Device>	The storage medium is displayed.
Boot device	This shows whether the device has booted from this storage medium.
Volume name	The name of the storage medium is displayed.

“Create new Filesystem on Memory Card” Group

Table 92: WBM “Mass Storage” Page – “Create new Filesystem on Memory Card” Group

Parameter	Meaning	
Filesystem type	You can select the format in which the filesystem should be created on the memory card.	
	Ext4	The filesystem is created in Ext4 format. The files are not readable under Windows!
	FAT	The filesystem is created in FAT format.
Label	Specify the name for the storage medium when formatted.	



Note

Data is deleted!
Any data stored in the storage medium is deleted during formatting!

To format the specified storage medium, click **[Start]**.

16.1.1.2.13 “Software Uploads” Page

On “Software Upload” page, you can install software packages on the product from your PC.

Table 93: WBM “Software Uploads” Page – “Upload New Software” Group

Parameters	Explanation
Software file	The file name of your selected software package is displayed, as long as you have not yet transferred it to the product. If you have not yet selected a package, “Choose ipk file...” appears. Click the input field and select a file with a software package on your PC.

To install the package, click **[Install]**.

The file with the software package is deleted from the device again after the installation process. If this is not possible due to a processing error, it is deleted no later than the next time the product restarts.

16.1.1.2.14 “Configuration of Network Services” Page

The settings for various services are shown on the “Configuration of Network Services” page.



Note

Close any ports and services that you do not need!
Unauthorized persons may gain access to your automation system through open ports.
To reduce the risk of cyber attacks and thus increase cyber security, close all ports and services not required by your application in the control components (e.g., port 6626 for WAGO-I/O-*CHECK*, port 2455 for CODESYS V2 and port 11740 for ***e!****COCKPIT*).
Only open ports and services during commissioning and/or configuration.

“FTP” Group

Table 94: WBM “Configuration of Network Services” Page – “FTP” Group

Parameters	Explanation
Service active	Enable/disable the FTP service. This service is disabled by default.

Click the **[Submit]** button to apply a change. The change takes effect immediately.

“FTPES (explicit FTPS)” Group

Table 95: WBM “Configuration of Network Services” Page – “FTPS (explicit FTPS)” Group

Parameters	Explanation
Service active	Enable/disable the FTPS service. This service is disabled by default.

Click the **[Submit]** button to apply a change. The change takes effect immediately.

“HTTP” Group

Table 96: WBM “Configuration of Network Services” Page – “HTTP” Group

Parameters	Explanation
Service active	Enable/disable the HTTP service. This service is disabled by default.

Click the **[Submit]** button to apply a change. The change takes effect immediately.



Note

Disconnection abort on disabling

If the HTTP service is disabled, the connection to the product may be interrupted. In that case, reopen the page.

“HTTPS” Group

Table 97: WBM “Configuration of Network Services” Page – “HTTPS” Group

Parameters	Explanation
Service active	This displays the status (enabled/disabled) of the HTTPS service.

“I/O-*CHECK*” Group

Table 98: WBM “Configuration of Network Services” Page – “I/O-*CHECK*“ Group

Parameters	Explanation
Service active	Enable/disable the WAGO-I/O-*CHECK* service.

Click the **[Submit]** button to apply a change. The change takes effect immediately.

16.1.1.2.15 “Configuration of NTP Client” Page

The settings for the NTP service are shown on the “Configuration of NTP Client” page.

“NTP Client Configuration” Group

Table 99: WBM “Configuration of NTP Client” Page – “NTP Client Configuration” Group

Parameters	Explanation
Service enabled	Enable/disabled time update.
Update interval (sec)	Specify the update interval of the time server.
Time Server <n>	Enter here the IP addresses of up to 4 time servers. Time server No. 1 is queried first. If no data is accessible via this server, time server No. 2 is queried, etc.
Additionally assigned (DHCP)	The NTP servers assigned if necessary by DHCP (or BootP) are displayed. If no NTP server has been assigned by DHCP (or BootP), “(No additional servers assigned)” is displayed.

To update the time regardless of interval, click the **[Update Time]** button.

Click the **[Submit]** button to apply the changes. The changes take effect immediately.

16.1.1.2.16 “PLC Runtime Services” Page

The settings for various services of the runtime systems are displayed on the “PLC Runtime Services” page.

“CODESYS V2” Group

This group only appears if the controller supports the CODESYS V2 runtime system.

Table 100: WBM “PLC Runtime Services” Page – “CODESYS V2” Group

Parameter	Explanation
CODESYS 2 State	This displays the status (enabled/disabled) of the CODESYS V2 runtime system.
Webserver enabled	Enable or disable the CODESYS V2 Webserver for the CODESYS web visualization.
Communication enabled	Enable or disable the communication between the CODESYS V2 runtime system and the CODESYS V2 programming system.
Communication Port Number	Enter here the port number for communication with the CODESYS V2 programming system. The default value is 2455.
Port authentication enabled	Define here whether port authentication is enabled. If this is enabled, the password specified under “General Configuration” must be entered when logging in via CODESYS V2 IDE.

Click the **[Submit]** button to apply the change.
The change in authentication takes effect after the next restart.
All other changes take effect immediately.

“*e!RUNTIME*” Group

This group only appears if the controller supports the ***e!****RUNTIME* runtime system.

Table 101: WBM “PLC Runtime Services” Page – “***e!****RUNTIME*” Group

Parameter	Explanation
e!*RUNTIME* State	This displays the status of the ***e!****RUNTIME* system (enabled/disabled).
Webserver enabled	Enable or disable the Webserver for the ***e!RUNTIME*** web visualization.
Port authentication enabled	Enter here whether a login is required for connecting to the device. The user name is admin and the password specified at “General Configuration.”

Click the **[Submit]** button to apply the change.
The change in authentication takes effect after the next restart.
All other changes take effect immediately.

16.1.1.2.17 “SSH Server Settings” Page

The settings for the SSH service are shown on the “SSH Server Settings” page.

“SSH Server” Group

Table 102: WBM “SSH Server Settings” Page – “SSH Server” Group

Parameters	Explanation
Service active	You can enable/disable the SSH server.
Port Number	Enter the port number.
Allow root login	You can enable or inhibit root access.
Allow password login	Enable or disable the password query function.

Click the **[Submit]** button to apply the changes. The changes take effect immediately.

16.1.1.2.18 “DHCP Server Configuration” Page

The “DHCP Server Configuration” page displays the DHCP service settings.

“DHCP Server Configuration Bridge <n>” Group

Table 103: WBM “DHCP Server Configuration” Page – “DHCP Configuration Bridge <n>” Group

Parameter	Explanation
Service active	Enable or disable the DHCP service for the interface X<n>.
Start IP for Range	Enter the start value of the available IP address range.
End IP for Range	Enter the end value of the available IP address range.
Lease time (min)	Specify the lease time here in seconds. 120 minutes are entered by default.
Static Hosts	This displays the static assignments of MAC IDs to IP addresses. If no assignment was defined, “No static hosts configured” is displayed.
Add Static Host	You can add static MAC addresses or host names and IP addresses.
MAC Address or Hostname	Enter a new static assignment, e.g., “01:02:03:04:05:06=192.168.1.20” or “hostname=192.168.1.20”. You can enter 15 assignments or host names.
Ip Address	Enter the IP address. You can enter 15 IP addresses.

Click the **[Submit]** button to apply the changes. The changes take effect immediately.

To accept a new assignment click the **[Add]** button. The change takes effect immediately.

Click **[Delete]** to delete an existing assignment. The change takes effect immediately.

16.1.1.2.19 “Configuration of DNS Server” Page

The “Configuration of DNS Server” page displays the DNS service settings.

“DNS Server” Group

Table 104: WBM “Configuration of DNS Server” Page – “DNS Server” Group

Parameter	Explanation	
Service active	You can enable/disable the DNS server service.	
Mode	Select the operating mode of the DNS server.	
	Proxy	Requests are buffered to optimize throughput.
	Relay	All requests are routed directly.
Static Hosts	This displays the names for IP addresses. If no assignment was defined, “No static hosts configured” is displayed.	
Add Static Host	You can add static IP addresses and host names below.	
IP Address	Enter a new static assignment, e.g., “192.168.1.20:hostname”. You can enter 10 assignments.	
Hostname	Enter a host name.	

Click the **[Submit]** button to apply the changes. The changes take effect immediately.

To accept a new assignment click the **[Add]** button. The change takes effect immediately.

Click **[Delete]** to delete an existing assignment. The change takes effect immediately.

16.1.1.2.20 “Status overview” Page

On the “Status overview” page, you can find information about cloud access.

“Service” Group

Table 105: WBM “Status Overview” Page – “Service” Group

Parameter	Explanation
Version	The cloud plug-in version is displayed.

“Connection <n>” Group

A group is displayed for each cloud access.

Table 106: WBM “Status Overview” Page – “Connection <n>” Group

Parameter	Explanation
Operation	The status of the cloud connectivity application is displayed.
Data from PLC Runtime	This shows how many data collections have been registered on the IEC application side for transfer to the cloud.
Cloud Connection	The status of the connection to the cloud service is shown.
Heartbeat	This shows the current heartbeat interval setting in seconds.
Telemetry Data Transmission	This indicates whether transfer of data is enabled or disabled.
Cache fill level (QoS 1 and 2)	This shows the fill level of the memory cache for outgoing messages as a percentage.

16.1.1.2.21 “Configuration of Connection <n>” Page

You can find settings and information for cloud access on the “Configuration of Connection <n>” page.

A page is displayed for each cloud access.

“Configuration” Group

The parameters indicated depend on the cloud platform setting and, if applicable, on other settings in this group.
The dependencies are shown in a separate table.

Table 107: WBM “Configuration of Connection <n>” Page – “Configuration” Group

Parameter	Explanation
Enabled	You can enable/disable the cloud connectivity function.
Cloud platform	Select the cloud platform.
Hostname	Enter the host name or IP address for the selected cloud platform.
Port number	Enter the port here to which a connection is to be established. Typical values are 8883 for encrypted connections and 1883 for unencrypted connections.
Device ID	Enter the device ID for the selected cloud platform.
Client ID	Enter the client ID for the selected cloud platform.
Authentication	Select the authentication method. Possible settings are “Shared Key Access” or “X.509 Certificate”.
Activation Key	Enter the activation key for the selected cloud platform.
Clean Session	Specify whether clean session should be enabled during the connection to the cloud service. If clean session is enabled, the information and messages on this connection are not stored persistently on the cloud service.
TLS	You can specify whether TLS encryption should be used for the connection to the cloud platform. Amazon Web Services (AWS) always uses TLS.
CA file	Enter the path here to the file encoded in PEM format that contains the trusted CA certificate to use to establish an encrypted connection. The default value is the CA certificate /etc/ssl/certs/ca-certificates.crt that is already installed on the controller.
Users	Enter the user name for cloud service authentication.
Password	Enter the password for cloud service authentication.

Table 107: WBM “Configuration of Connection <n>” Page – “Configuration” Group

Parameter	Explanation
Certification file	Enter the path here to the file encoded in PEM format that is used for cloud service authentication.
Key file	Enter the path to the file encoded in PEM format that contains the private key for cloud service authentication.
Use websockets	Here, you can specify whether the connection to the cloud platform is to be set up using the Websocket protocol via Port 443. If this checkbox is not selected, the connection to the cloud platform is set up using the MQTT protocol via Port 8883.
Proxy Type	Select which type of proxy should be used.
HTTP Proxy Host	Enter the host name or IP address of the proxy.
HTTP Proxy Port	Enter the port number of the proxy.
HTTP Proxy User	Enter the name of the proxy user.
HTTP Proxy Password	Enter the password for the proxy user.
Use compression	Here, you can set whether the data is to be compressed using GZIP compression.
Data Protocol	Here you can select the data protocol.
Cache mode	Specify in which memory the cache for the data telegrams should be created. This selection field is only enabled if a correctly formatted SD card is inserted (more information is available in Application Note A500920).
Last Will	You can specify whether a last will message should be enabled/disabled.
(Last Will) Topic	You can specify the topic under which the last will messages should be sent.
(Last Will) Message	You can enter the message you wish to use as the last will message.
(Last Will) QoS	You can specify the “Quality of Service” (QoS) of the last will message.
(Last Will) Retain	Here, you can set whether the previous last-will message sent under a topic from the broker is to be handled as a retained message.
Device info	Specify whether a device info message should be generated that informs the cloud service of the basic configuration of the controller (more information is available in the Application Note A500920).
Device status	Specify whether device state messages should be generated that inform the cloud service about changes in the mode selector switch and the LEDs (more information is available in the Application Note A500920).

Table 107: WBM “Configuration of Connection <n>” Page – “Configuration” Group

Parameter	Explanation
Standard commands	Specify whether the integrated standard commands should be supported (list of standard commands is available in the Application Note A500920). If the checkbox is disabled, only the commands defined in the IEC program are supported.
Application property template	You have the option of creating your own property for the individual MQTT messages to the Azure cloud. This parameter is optional; i.e., if the field is left blank, this property is not sent. The following placeholders are available to create this property: • <m>: Message type • <p>: Protocol version • <d>: Device ID Examples: • MyKey=HelloWorld_<m> • TestKey=<m>/<p>/<d> • DeviceId=<d>

Click the **[Submit]** button to apply a change.

The changes only take effect after the controller restarts. For this purpose, use the WBM reboot function. Do not shut down the controller too early!

The following tables show the dependencies of the selection and input fields as well as the possible settings.

Table 108: Display of the Selection and Input Fields Depending on the Selected Cloud Platform

Selection or Input Field	Cloud Platform					
	WAGO Cloud	Azure	MQTT AnyCloud	IBM Cloud	Amazon Web Services	SAP IoT Services
Enabled	X	X	X	X	X	X
Cloud platform	X	X	X	X	X	X
Hostname	X	X	X	X	X	X
Port number			X	X	(X)	X
Device ID	X	X				
Client ID			X	X	X	X
Authentication		X				
Activation Key	X	X2				
Clean Session			X	(X)	(X)	X
TLS			X	X	(X)	X
CA file			X	X	X	X

Table 108: Display of the Selection and Input Fields Depending on the Selected Cloud Platform

Selection or Input Field	Cloud Platform					
	WAGO Cloud	Azure	MQTT AnyCloud	IBM Cloud	Amazon Web Services	SAP IoT Services
User			X	X		
Password			X	X		
Certification file		X2	X		X	X
Key file		X2	X		X	X
Use websockets	X	X1				
Proxy Type	X4	X4				
HTTP Proxy Host	X5	X5				
HTTP Proxy Port	X5	X5				
HTTP Proxy User	X5	X5				
HTTP Proxy Password	X5	X5				
Data Protocol		X	X	X	X	(X)
Use compression	X	X1	X1			
Cache mode	X	X	X	X	X	X
Last Will			X	X	X	X
Last Will Topic			X3	X3	X3	X3
Last Will Message			X3	X3	X3	X3
Last Will QoS			X3	X3	X3	X3
Last Will Retain			X3	X3	(X3)	X3
Device info		X1	X1	X1	X1	
Device status		X1	X1	X1	X1	
Standard commands		X1	X1		X1	
Application property template		X1				

X: Visible and enabled
(X): Visible, but disabled
X1: Visible and enabled, depending on the selected data protocol
X2: Visible and enabled, depending on the selected authentication
X3: Visible and enabled when “Last Will” is switched on
(X3): Visible, but disabled when “Last Will” is switched on
X4: Enabled if “Use websockets” is switched on.
X5: Visible and enabled if “Use websockets” is switched on and if “HTTP” is set as the “Proxy Type”.

Table 109: Choice of Data Protocol Depending on the Selected Cloud Platform

Data Protocol	Cloud Platform					
	WAGO Cloud	Azure	MQTT AnyCloud	IBM Cloud	Amazon Web Services	SAP IoT Services
WAGO Protocol		X	X	X	X	
WAGO Protocol 1.5		X	X	X	X	
Native MQTT			X	X	X	(X)
Sparkplug payload B		X	X		X	

X: Selection possible
(X): Fixed setting

Table 110: Display of the Selection and Input Fields Depending on the Selected Data Protocol

Selection or Input Field	Data Protocol			
	WAGO Protocol	WAGO Protocol 1.5	Native MQTT	Sparkplug payload B
Client ID	X	X	X	X
Use compression	X	X	X	
Device info	X	X		
Device status	X	X		
Standard commands	X	X		
Application property template	X	X		

X: Visible and enabled

Table 111: Choice of Cache Mode Depending on the Selected Data Protocol

Cache Mode	Data Protocol			
	WAGO Protocol	WAGO Protocol 1.5	Native MQTT	Sparkplug payload B
RAM	X	X	X	(X)
SD-Card	X1	X1	X1	

X: Selection possible
X1: Selection only possible if “Compression” is not switched on
(X): Fixed setting

Table 112: Display of the Selection and Input Fields Depending on the Selected Authentication

Selection or Input Field	Authentication	
	Shared Access Key	**X.509 Certificate**
Activation Key	X	
Certification file		X
Key file		X

X: Visible and enabled

16.1.1.2.22 “Configuration of General SNMP Parameters” Page

The general settings for SNMP are given on the “Configuration of General SNMP Parameters” page.

“General SNMP Configuration” Group

Table 113: WBM “Configuration of General SNMP Parameters” Page – “General SNMP Configuration” Group

Parameter	Explanation
Service active	Activate/deactivate the SNMP service.
Name of device	Enter here the device name (sysName).
Description	Enter here the device description (sysDescription).
Physical location	Enter here the location of the device (sysLocation).
Contact	Enter here the email contact address (sysContact).
Object ID	Enter here the object ID (sysOID).

Click the **[Submit]** button to apply the changes. The changes only take effect after restarting the controller. For this purpose, use the WBM reboot function. Do not shut down the controller too early!

16.1.1.2.23 “Configuration of SNMP v1/v2c Parameters” Page

The general settings for SNMP v1/v2c are shown on the “Configuration of SNMP v1/v2c Parameters” page.

“SNMP v1/v2c Manager Configuration” Group

Table 114: WBM “Configuration of SNMP v1/v2c Parameters” Page – “SNMP v1/v2c Manager Configuration” Group

Parameters	Explanation
Protocol enabled	It is displayed the SNMP protocol for v1/v2c is enabled. The local community name is deleted when the protocol is disabled.
Local Community Name	Specify the community name for the SNMP manager configuration. The community name can establish relationships between SNMP managers and agents who are respectively referred to as “Community” and who control identification and access between SNMP participants. The community name can be up to 32 characters long and must not include spaces. To use the SNMP protocol, a valid community name must always be specified. The default community name is “public.”

Click the **[Submit]** button to apply the changes. The changes only take effect after the controller restarts. For this purpose, use the WBM reboot function. Do not shut down the controller too early!

“Actually configured Trap Receivers” Group

Table 115: WBM “Configuration of SNMP v1/v2c Parameters” Page – “Actually Configured Trap Receivers” Group

Parameters	Meaning
Each configured trap receiver has its own area in the display. If no trap receiver has been configured, “(no trap receivers configured)” is displayed.	
IP Address	The IP address for the trap receiver (management station) is displayed.
Community Name	This displays the community name for the trap receiver configuration. The community name can be evaluated by the trap receiver.
Version	This displays the SNMP version, via which the traps are sent: v1 or v2c (traps higher than v3 are displayed in a separate form).
Add new Trap Receiver	In this area, you can enter a new trap receiver.
IP Address	Specify the IP address for the new trap receiver (management station).
Community Name	Specify the community name for the new trap receiver configuration. The community name can be evaluated by the trap receiver. The community name can be up to 32 characters long and must not include spaces.
Version	Specify the SNMP version that will send the traps: v1 or v2c (traps higher than v3 are configured in a separate form).

Click the corresponding **[Delete]** button to delete an existing trap receiver.

Click the **[Add]** button to add a new trap receiver.

The changes only take effect after the controller restarts. For this purpose, use the WBM reboot function. Do not shut down the controller too early!

16.1.1.2.24 “Configuration of SNMP v3 Users” Page

The general settings for SNMP v3 are shown on the “Configuration of SNMP v3 Users” page.

“Actually configured v3 Users” Group

Table 116: WBM “Configuration of SNMP v3” Page – “Actually configured v3 Users” Group

Parameters	Meaning
User <n>	Each configured v3 user has its own area in the display. If no v3 user has been configured, “(no trap receivers configured)” is displayed.
Security Authentication Name	The user name is displayed.
Authentication Type	The authentication type for the SNMP v3 packets is displayed. Possible values: - Use no authentication (“None”) - Message Digest 5 (“MD5”) - Secure Hash Algorithm (“SHA”)
Authentication Key	The authentication key is displayed.
Privacy	The encryption algorithm for the SNMP message is displayed. Possible values: - No encryption (“None”) - Data Encryption Standard (“DES”) - Advanced Encryption Standard (“AES”)
Privacy Key	The key for encryption of the SNMP message is displayed. If nothing is displayed, the “authentication key” is automatically used.
Notification Receiver IP	The IP address of a trap receiver for v3 traps is displayed. If no v3 traps are to be sent for this user, this field remains blank.
Add new v3 User	In this area, you can enter a new v3 user. You can create up to 10 users.
Security Authentication Name	Enter the user name. This name must be unique; a pre-existing user name is not accepted when entered. The name must be min. 8 and max. 32 characters long and contain lower case letters (a … z), upper case letters (A … Z), numbers (0 … 9), special characters !()*~'.-_ but no spaces.

Table 116: WBM “Configuration of SNMP v3” Page – “Actually configured v3 Users” Group

Parameters	Meaning
Authentication Type	Specify the authentication type for the SNMP v3 packets. Possible values: - Use no authentication (“None”) - Message Digest 5 (“MD5”) - Secure Hash Algorithm (“SHA”)
Authentication Key (min. 8 char.)	Specify the authentication key. The key must be min. 8 and max. 32 characters long and contain lower case letters (a … z), upper case letters (A … Z), numbers (0 … 9), special characters !()*~'.-_ but no spaces.
Privacy	Specify the encryption algorithm for the SNMP message. Possible values: - No encryption (“None”) - Data Encryption Standard (“DES”) - Advanced Encryption Standard (“AES”)
Privacy Key (min. 8 char.)	Enter the key for encryption of the SNMP message. If nothing is specified here, the “authentication key” is automatically used. The key must be min. 8 and max. 32 characters long and contain lower case letters (a … z), upper case letters (A … Z), numbers (0 … 9), special characters !()*~'.-_ but no spaces.
Notification Receiver IP	Specify an IP address for a trap receiver for v3 traps. If no v3 traps are to be sent for this user, this field remains blank.

Click the respective **[Delete]** button to delete an existing user.

Click **[Add]** to add a new user.

The changes only take effect after the controller restarts. For this purpose, use the WBM reboot function. Do not shut down the controller too early!

16.1.1.2.25 “WBM User Configuration” Page

The settings for user administration are displayed on the “WBM User Configuration” page.

“Change Password” Group



Note

Changing Passwords
The initial passwords as delivered are documented in this manual and therefore do not provide sufficient protection. Change the passwords to meet your particular needs!

Table 117: WBM “WBM User Configuration” Page – “Change Password” Group

Parameter	Explanation
Old Password	Enter the current password here for authentication.
New Password	Enter the new password here. Permitted characters for the password are the following ASCII characters: a … z, A … Z, 0 … 9, blank spaces and special characters: ! ? % + = ( ) _ # " - / ` < > * ; , : .
Confirm Password	Enter the new password again here for confirmation.

Click the **[Submit]** button to apply a change. The change takes effect immediately.



Note

Note the permitted characters for WBM passwords!
If passwords with invalid characters are set for the WBM outside the WBM (e.g., from a USB keyboard), access to the pages directly on the display is no longer possible because only permitted characters are available from the virtual keyboard.



Note

General Rights of WBM Users
The WBM users “admin” and “user” have rights beyond the WBM to configure the system and install software.

User administration for controller applications is configured and managed separately.

16.1.1.3 “Fieldbus” Tab

16.1.1.3.1 “OPC UA Status” Page

You can find the status information on the OPC UA service on the “OPC UA Status” page.

“OPC UA Server” Group

Table 118: WBM “OPC UA Status” Page – “OPC UA Server” Group

Parameter	Explanation
State	The current status (enabled / disabled) of the WAGO OPC UA server is displayed.
Version	The installed version of the WAGO OPC UA Server is displayed here.
License	Any existing OPC UA server license is displayed. Some features of the WAGO OPC UA server require a paid special license.

16.1.1.3.2 “OPC UA Configuration” Page

The settings for the OPC UA service are shown on the “OPC UA Configuration” page.

“General OPC UA Server Configuration” Group

Table 119: WBM “OPC UA Configuration” Page – “General OPC UA Server Configuration” Group

Parameter	Explanation	
Service enabled	Enable or disable the WAGO OPC UA Server here.	
Ctrl Configuration name	Enter the configuration names the controller contains in the PLC Open Device Set.	
Log level	Select the log level. The following values can be set: Info / Debug / Warning / Error. With log level “Error,” only error messages are read out; with log level “Info,” status messages are read out too. The specific log level selection affects server reaction time. Therefore, select the lowest level necessary; e.g., “Debug” for in-depth analyses.	
Unlimited anonymous access	Access rights to the data provided by the server are set here.	
	Enabled	An unregistered user can view, read and write all variables.
	Disabled	Complete access to the data requires user logon with the appropriate rights.

Click the **[Submit]** button to apply the changes.

Group “OPC UA Endpoint URL”

Table 120: WBM page “OPC UA Configuration” – group “OPC UA Endpoint URL”

Parameter	Meaning
Interface	Select the endpoint URL of the OPC UA server. The hostname or a bridge or IP address is possible.

“OPC UA Endpoints” Group

Table 121: WBM “OPC UA Configuration” Page – “OPC UA Endpoints” Group

Parameter	Meaning
Security Policy - None	Enable or disable the OPC UA endpoint “None”. This allows an unsecured connection to the OPC UA server to be established.
Security Policy - Basic128Rsa15	Enable or disable the “Basic128Rsa15” security policy. **Note:** This policy is no longer classified as secure.
Security Policy - Basic256Sha256	The “Basic256Sha256” security policy allows a secure connection to be established with the OPC UA server.

Click the **[Submit]** button to apply the changes.

“OPC UA Security Settings” Group

Table 122: WBM Page “OPC UA Configuration” – “OPC UA Security Settings” Group

Parameter	Explanation	
Trust all clients	The verification is enabled or disabled here.	
	Enabled	A connection to all clients is permitted. → No security!
	Disabled	Connection is only allowed to clients with secure certificates.
URI Check Application	The URI check can be enable or disable here. A disabled URI check enables connection to an OPC server even if the URI on the server URI is different from the URI in the certificates.	
Error Certificate Time	The time can be enabled or disabled here. Certificates may have an expiration date. This date is checked against the current usage time on the device. The check cannot be run successfully if the time is incorrectly set on the device.	
Certificate Issuer Time Invalid	The time stamp check can be enabled or disabled here. CA certificates contain a validity time stamp from the manufacturer. This stamp is used when checking the time on the server hardware. If the time setting on the server hardware is incorrect or is missing entirely, the certificate may be indicated as invalid.	
Certificate Revocation Unknown	The accessibility check of the saving location for withdrawn certificates can be enabled or disabled here. Each certificate can have a location for withdrawn certificates. If network problems or other causes prevent access to the specified location, the certificate is not accepted.	
Certificate Issuer Revocation Unknown	The accessibility check of the storage location for withdrawn certificates can be enabled or disabled here. Each certificate of a certification location (CA certificate) can contain an entry for the withdrawn certificate saving location. If the location cannot be reached, the server will refuse the certificate.	

Click the **[Submit]** button to apply the changes.

16.1.1.3.3 “OPC UA Server Certificates” Page

The “OPC UA Server Certificates” provides options to install or delete OPC UA server certificates and keys.

“OPC UA Server Own Certificate” Group

Table 123: WBM Page “OPC UA Server Certificates” – “OPC UA Server Own Certificate” Group

Parameter	Meaning
<certificate name> e.g., “certificate.der”	The certificate currently used by the server is displayed. If no certificate is being used, “No certificates existing” is displayed.

To delete the certificate, click the **[Delete]** button. The change applies immediately.

To select a certificate file on the PC, click the **Choose file …** selection field.

To transfer the selected certificate file to the product, click the **[Upload]** button. The change applies immediately.

“OPC UA Server Private Keys” Group

Table 124: WBM Page “OPC UA Server Certificates” – “OPC UA Server Private Keys” Group

Parameter	Meaning
<private key name> e.g., “key.pem”	The key currently used is displayed. If not key has been loaded, “No private keys existing” is displayed.

To delete the key, click the **[Delete]** button. The change applies immediately.

To select a key file on the PC, click the **Choose file …** selection field.

To transfer the selected key file to the product, click the **[Upload]** button. The change applies immediately.

“OPC UA Server Trusted / Rejected Certificates” Group

Table 125: WBM Page “OPC UA Server Certificates” – “OPC UA Server Trusted / Rejected Certificates” Group

Parameter	Meaning
Trusted	The certificates of clients marked as trustworthy are listed in this area. If not certificate exists, “No certificates existing” is displayed.
Rejected	This area lists the certificates of OPC UA devices that have not yet been classified as trustworthy or that have been marked as “Rejected”. If not certificate exists, “No certificates existing” is displayed.

To move a certificate from the “Trusted” area to the “Rejected” area, click the **[Reject]** button. The change applies immediately.

To delete a certificate, click the **[Delete]** button. The change applies immediately.

To select a certificate file on the PC, click the **Choose file …** selection field.

To transfer the selected certificate file to the product, click the **[Upload]** button. The change applies immediately. The loaded certificate is first listed in the “Rejected” area.

16.1.1.3.4 “MODBUS Services Configuration” Page

The “Modbus Services Configuration” page displays the settings for various Modbus® services. The groups only appear if the ***e!****RUNTIME* system is enabled. Otherwise an information text is displayed.

“Modbus TCP Slave” Group

Table 126: WBM “Modbus Services Configuration” Page – “Modbus TCP” Group

Parameters	Explanation
Service active	Disable or enable the Modbus/TCP service.

Click the **[Submit]** button to apply the changes. The change takes effect immediately.

“Modbus UDP Slave” Group

Table 127: WBM “Modbus Services Configuration” Page – “Modbus UDP” Group

Parameters	Explanation
Service active	Disable/enable the Modbus UDP service.

Click the **[Submit]** button to apply the changes. The change takes effect immediately.

16.1.1.4 “Security” Tab

16.1.1.4.1 “OpenVPN / IPsec Configuration” Page

The “OpenVPN / IPsec Configuration” page displays the settings for OpenVPN and IPsec.

“OpenVPN” Group

Table 128: WBM “OpenVPN / IPsec Configuration” Page – “OpenVPN” Group

Parameter	Explanation	
Current State	The current status of the OpenVPN service is displayed.	
	stopped	The service is disabled.
	running	The service is enabled.
OpenVPN enabled	Enable or disable the OpenVPN service.	
openvpn.config	Select an OpenVPN configuration file to be transferred from PC to product or vice versa.	

Click the **[Submit]** button to apply a change.

To select a file on the PC, click the **Choose file …** selection field.

To transfer the selected file from the PC to the product, click **[Upload]** button.

To transfer a file from product to PC, click the **[Download]** button.

The changes only take effect after the product restarts. For this purpose, use the WBM reboot function. Do not switch off the product too early!

“IPsec” Group

Table 129: WBM “OpenVPN / IPsec Configuration” Page – “IPsec” Group

Parameter	Explanation	
Current State	The current status of the IPsec service is displayed.	
	stopped	The service is disabled.
	running	The service is enabled.
IPsec enabled	Enable or disable the IPsec service.	
ipsec.conf	Select an IPsec configuration file to be transferred from PC to product or vice versa.	
ipsec.secrets	Select an IPsec configuration file to be transferred from PC to product or vice versa.	

Click the **[Submit]** button to apply a change.

To select a file on the PC, click the **Choose file …** selection field.

To transfer the selected file from the PC to the product, click **[Upload]** button.

To transfer a file from product to PC, click the **[Download]** button.

The changes only take effect after the product restarts. For this purpose, use the WBM reboot function. Do not switch off the product too early!

16.1.1.4.2 “General Firewall Configuration” Page

The “General Firewall Configuration” page displays the global firewall settings.

“Global Firewall Parameter” Group

Table 130: WBM “General Firewall Configuration” Page – “Global Firewall Parameter” Group

Parameter	Explanation
Firewall enabled entirely	Enables/disables the complete functionality of the firewall. This setting has the highest priority. If the firewall is disabled, all other settings have no direct effect. The configuration of the other parameters is possible nevertheless so that you can set the firewall parameters correctly before you enable the firewall. This setting is independent of the “Filter enabled” setting in the “MAC address filter state bridge <n>” group on the “MAC address filter state bridge <n>” page.
ICMP echo broadcast protection	Enable or disable the “ICMP echo broadcast” protection.
Max. UDP connections per second	You can specify the maximum number of UDP connections per second.
Max. TCP connections per second	You can specify the maximum number of TCP connections per second.

Click **[Submit]** to apply the change. The change takes effect immediately.

16.1.1.4.3 “Interface Configuration” Page

The individual interfaces for the firewall settings are displayed on the “Interface Configuration” page.

“Firewall Configuration Bridge <n> / VPN / WAN” Group

A separate group is displayed for each configured bridge.
The settings in this group are based on the firewall configuration on the IP level.

Table 131: WBM “Interface Configuration” Page – “Firewall Configuration Bridge <n> / VPN / WAN” Group

Parameter	Explanation	
Firewall enabled for Interface	Enable or disable the firewall for the respective bridge.	
ICMP echo protection	Enable or disable the “ICMP echo” protection for the respective bridge.	
ICMP echo limit per second	You can specify the maximum number of “ICMP pings” per second. “0” = “Disabled”	
ICMP burst limit (0 = disabled)	You can specify the maximum number of “ICMP echo bursts” per second. “0” = “Disabled”	
Service enabled	FTP/FTPES	Enable or disable the firewall for the respective service. The services themselves must be enabled or disabled separately on the “Ports and Services” page.
	FTPS (implicit)	
	HTTP	
	HTTPS	
	I/O-CHECK	
	PLC Runtime	
	PLC WebVisu – direct link (port 8080)	
	SSH	
	BootP/DHCP	
	DNS	
	Modbus TCP	
	Modbus UDP	
	SNMP	
	OPC UA	
	BACnet (Port 47808)	
	PROFINET IO	
	DNP3 (port 20000)	
	IEC60870-5-104 (port 2404)	
	IEC61850 (port 102)	

Click the **[Submit]** button to apply the change. The change takes effect immediately.

16.1.1.4.4 “Configuration of MAC Address Filter” Page

The “Configuration of MAC address filter” page displays the firewall configuration on the ETHERNET level.

The “MAC Address Filter Whitelist” contains a default entry with the following values:

MAC address: 00:30:DE:00:00:00
MAC mask: ff:ff:ff:00:00:00

If you enable the default entry, this already allows communication between different WAGO devices in the network.



Note

Enable the MAC address filter before activation!
Before activating the MAC address filter, you must enter and activate your own MAC address in the “MAC Address Filter Whitelist.”
Otherwise you cannot access the device via the ETHERNET. This also applies to other services that are used by your device, e.g., the IP configuration via DHCP.
If the “MAC Address Filter Whitelist” does not contain the MAC address of your DHCP server, your device will lose its IP settings after the next refresh cycle and is then no longer accessible.
If the “MAC Address Filter Whitelist” does not contain an entry, the activation of the filter is prevented.
If at least one enabled address is entered, you will receive an appropriate warning before activation, which you have to acknowledge.
The check described above is only performed in the WBM but not in the CBM!

“Global MAC address filter state” Group

Table 132: WBM “Configuration of MAC Address Filter” Page – “Global MAC address filter state” Group

Parameters	Explanation
Filter enabled	Enable or disable the global MAC address filter.

Click the **[Submit]** button to apply the change. The change takes effect immediately.

“MAC address filter state Bridge <n>” Group

A separate group is displayed for each configured bridge.

Table 133: WBM “Configuration of MAC Address Filter” Page – “MAC address filter state Bridge <n>” Group

Parameter	Explanation
Filter enabled	Enable or disable here the MAC address filter for the specific bridge. This setting is independent of the “Firewall enabled entirely” setting on the General Firewall Configuration page.

Click the **[Submit]** button to apply the change. The change takes effect immediately.

“MAC address filter whitelist” Group

Each list entry has its own area in the display.

Table 134: WBM “Configuration of MAC Address Filter” Page – “MAC address filter whitelist” Group

Parameters	Explanation
MAC address	Displays the MAC address of the relevant list entry.
MAC mask	This displays the MAC mask of the relevant list entry.
Filter enabled	Enable or disable the filter for the relevant list entry.
Add filter to whitelist	Create a new list entry.
MAC address	Enter here the MAC address for a new list entry. You can enter 10 filters.
MAC mask	Enter the MAC mask for the new list entry.
Filter enabled	Enable or disable the filter for the new list entry.

Click the **[Submit]** button to apply the change. The change takes effect immediately.

Click the appropriate **[Delete]** button to remove an existing list entry. The change takes effect immediately.

Click **[Add]** to accept a new list entry. You can enter 10 filters. The change takes effect immediately.

16.1.1.4.5 “Configuration of User Filter” Page

The “Configuration of User Filter” page displays the settings for custom firewall filters.

“User filter” Group

Each configured filter has its own area in the display.

Table 135: WBM “Configuration of User Filter” Page – “User Filter” Group

Parameters	Meaning	
Policy	This displays whether the network participant is permitted or excluded by the filter.	
Source IP address	The source IP address for the respective filter is displayed.	
Source Netmask	This displays the source netmask for the respective filter.	
Source Port	The source port number for the respective filter is displayed.	
Destination IP address	The destination IP address for the respective filter is displayed.	
Destination Netmask	The destination netmask for the respective filter is displayed.	
Destination Port	The destination port number for the respective filter is displayed.	
Protocol	The permitted protocols for the respective filter is displayed.	
Input interface	The permitted interfaces for the respective filter are displayed.	
Add new user filter	You can create up to 10 filters. You only have to enter values in the fields that are to be set for the filter. At least one value must be entered, all other fields can remain empty.	
Policy	Select here whether the network devices is to be allowed or excluded by the filter.	
	Allow	The network device is permitted.
	Drop	The network device is excluded.
Source IP address	Enter here the source IP address for the new filter.	
Source netmask	Enter here the source network mask for the new filter.	
Source port	Enter here the source port address for the new filter.	
Destination IP address	Enter here the destination IP address for the new filter.	
Destination subnet mask	Enter here the destination network mask for the new filter.	
Destination port	Enter here the destination port address for the new filter.	

Table 135: WBM “Configuration of User Filter” Page – “User Filter” Group

Parameters	Meaning	
Protocol	Enter here the protocols for the new filter.	
	TCP/ UDP	The TCP service and UDP service are filtered.
	TCP	The TCP service is filtered.
	UDP	The UDP service is filtered.
Input interface	Enter here the interfaces for the new filter.	
	Any	All interfaces are filtered.
	Bridge <n>	The interfaces assigned for bridge <n> are filtered. Only the configured bridges are displayed.
	VPN	The VPN interface is filtered.

Click **[Add]** to apply the new filter. The change takes effect immediately.

Click the **[Delete]** button to delete an existing filter. The change takes effect immediately.

16.1.1.4.6 “Certificates” Page

On the “Certificates” page, you will find options to install or delete certificates and keys.

“Installed Certificates” Group

Table 136: WBM “Configuration of OpenVPN and IPsec” Page – “Certificate List” Group

Parameters	Explanation
<certificate name>	The loaded certificates are displayed. If no certificate has been loaded. “No certificates existing” is displayed.

To select a file on the PC, click the **Choose file …** selection field.

To transfer the selected file PC to the product, click the **[Upload]** button. The changes take effect immediately.

The certificates are stored in the directory “/etc/certificates/” and the keys in the directory “/etc/certificates/keys/”.

Click **[Delete]** to delete an entry. The changes take effect immediately.

“Installed Private Keys” Group

Table 137: WBM “Configuration of OpenVPN and IPsec” Page – “Private Key List” Group

Parameters	Meaning
<private key name>	The loaded keys are displayed. If no key has been loaded, “No private keys existing” is displayed.

To select a file on the PC, click the **Choose file …** selection field.

To transfer the selected file PC to the product, click the **[Upload]** button. The changes take effect immediately.

The certificates are stored in the directory “/etc/certificates/” and the keys in the directory “/etc/certificates/keys/”.

Click **[Delete]** to delete an entry. The changes take effect immediately.

16.1.1.4.7 “Security Settings” Page

The network security settings are found on the “Security Settings” page.

“TLS Configuration” Group

Table 138: “Security Settings” WBM Page – “TLS Configuration” Group

Parameters	Explanation	
TLS Configuration	You can set what TLS versions and cryptographic methods are allowed for HTTPS.	
	Standard	The Webserver allows TLS 1.0, TLS 1.1 and TLS 1.2, as well as cryptographic methods that are no longer considered secure.
	Strong	The Webserver only allows TLS Version 1.2 and strong algorithms. Older software and older operating systems may not support TLS 1.2.

Click the **[Submit]** button to apply a change. The change takes effect immediately.

Note

BSI TR-02102 Technical Guidelines
The rules for the “Strong” setting are based on the TR-02102 technical guidelines of the German Federal Office for Information Security (BSI).
You can find the guidelines on the Internet at: https://www.bsi.bund.de > “Publications” > “Technical Guidelines.”

16.1.1.4.8 “Advanced Intrusion Detection Environment (AIDE)” Page

The network security settings are available on the “Advanced Intrusion Detection Environment (AIDE)” page.

“Run AIDE check at startup” Group

Table 139: WBM “Advanced Intrusion Detection Environment (AIDE)” Page – “Run AIDE check at startup” Group

Parameter	Explanation
Service active	Here, you can activate/deactivate the “AIDE check” when the controller is started.

Click the **[Submit]** button to apply the changes. The changes only take effect when the controller restarts.

“Refresh Options” group

Table 140: WBM “Advanced Intrusion Detection Environment (AIDE)” Page – “Control AIDE and show log” Group

Parameter	Explanation	
Select Action	Select here the action to be executed.	
	readlog	The log data are displayed.
	init	The database is initialized and filled with the current values.
	check	The current values are compared against the values stored in the database.
	update	The current values are compared with the values stored in the database and the database then updated.
Read only the last n	Activate display of only the last n messages. You also specify the number of messages to be displayed.	
Automatic refresh interval (sec)	Select the checkbox to enable cyclic refresh. Enter the cycle time in seconds in which a cyclic refresh is performed. The label of the button (“Refresh”/“Start“/“Stop”) changes depending on status.	

Click **[Refresh]** to update the display. The button is only displayed if the cyclic refresh is not enabled.

To enable cyclic refresh, click the **[Start]** button. The button is only displayed if cyclic refresh is enabled and has not yet started.

To stop cyclic refresh again, click the **[Stop]** button. The button only appears if cyclic refresh is enabled.

The cyclical refresh is performed for as long as the “Advanced Intrusion Detection Environment (AIDE)” page is open. If you change the WBM page, the

update is stopped until you call up the “Advanced Intrusion Detection Environment (AIDE)” page again.

The messages are displayed below the settings.

16.1.1.5 “Diagnostic” Tab

16.1.1.5.1 “Diagnostic Information” Page

The settings for displaying diagnostic messages are shown on the “Diagnostic Information” page.

Table 141: WBM “Diagnostic Information” Page

Parameters	Meaning	
Read only the last	Activate display of only the last n messages. You also specify the number of messages to be displayed.	
Automatic refresh interval (sec)	Select the checkbox to enable cyclic refresh. Enter the cycle time in seconds in which a cyclic refresh is performed. The label of the button (“Refresh”/“Start“/“Stop”) changes depending on status.	
Source	Select the source of the diagnostic messages. The drop-down list depends on the user who is logged in.	
	user	Default diagnostic messages only
	admin	Default diagnostic messages and all log files in the folder `/var/log/*`

To refresh the display or to enable cyclic refresh, click the **[Refresh]** button. This button is only displayed if the cyclic refresh is not enabled.

To enable cyclic refresh, click the **[Start]** button. The button is only displayed if cyclic refresh is enabled and has not yet started.

To stop cyclic refresh again, click the **[Stop]** button. The button only appears if cyclic refresh is enabled.

The cyclical refresh is performed for as long as the “Diagnostic Information” page is open. If you change the WBM page, the refresh is stopped until you call up the “Diagnostic Information” page again.

The messages are displayed below the settings.

16.1.2 Console-Based-Management (CBM)

16.1.2.1 “Information” Menu

This menu contains other submenus with information on the controller and network.

Table 142: “Information” Menu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. Controller Details	Opens a submenu with controller properties
2. Network Details	Opens a submenu with controller network and interface properties

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

16.1.2.1.1 “Information” > “Controller Details” Submenu

In this submenu, the controller properties are displayed.

Table 143: “Information” > “Controller Details” Submenu

Parameters	Explanation
Product Description	Controller identification
Order Number	Item number of the controller
License Information	Notification that the CODESYS runtime system is available
Firmware Revision	Firmware status

To return to the higher-level menu, press **[Q]** or **[Return]**.

16.1.2.1.2 “Information” > “Network Details” Submenu

In this submenu, the network and interface properties of the controller are displayed.

If the EHERNET interfaces are operated in “Switched” mode, a common table (“X1/X2”) is displayed for both connections.
If the EHERNET interfaces are operated in “Separated” mode, an individual table (“X1” / “X2”) is displayed for each connection.

Table 144: “Information” > “Network Details” Submenu

Parameters	Explanation
State	Status of the ETHERNET interface (enabled/disabled)
Mac Address	MAC address identifies and addresses the controller
IP Address	Current IP address of the controller and (in brackets) the reference type (static/bootp/dhcp)
Subnet Mask	Current subnet mask of the controller

To return to the higher-level menu, press **[Q]** or **[Return]**.

16.1.2.2 “PLC Runtime” Menu

This menu contains other submenus with information and settings for the runtime system.

Table 145: “PLC Runtime” Menu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. Information	Opens a submenu with information on the runtime system
2. General Configuration	Opens a submenu with settings for the runtime system
3. WebVisu	Opens a submenu with settings for the Web visualization

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

16.1.2.2.1 “PLC Runtime” > “Information” Submenu

This submenu contains other submenus with information on the runtime system and PLC program.

Table 146: “PLC Runtime” > “Information” Submenu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. Runtime Version	Opens a submenu to display the runtime version

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

16.1.2.2.2 “Information” > “Runtime Version” Submenu

In this submenu, the runtime version is displayed.

Table 147: “PLC Runtime” > “Information” > “Runtime Version” Submenu

Parameters	Explanation
Version	The version of the currently enabled runtime system is shown. If the runtime system is disabled, “None” is displayed.

To return to the higher-level menu, press **[Q]** or **[Return]**.

16.1.2.2.3 “PLC Runtime” > “General Configuration” Submenu

This submenu contains other submenus with general settings for the runtime system.

Table 148: “PLC Runtime” > “General Configuration” Submenu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. PLC Runtime Version	Opens a submenu for the CODESYS runtime system settings
2. Home Dir On SD Card	Opens a submenu for the home directory settings

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

16.1.2.2.4 “General Configuration” > “PLC Runtime Version” Submenu

In this submenu, select which PLC runtime system is enabled.

Table 149: “PLC Runtime” > “General Configuration” > “PLC Runtime Version” Submenu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. None	No runtime system is enabled.
2. e!RUNTIME	The ***e!****RUNTIME* runtime system is enabled.



Note

All data is deleted when switching the runtime system!
The runtime system’s home directory is completely deleted when switching the runtime system!

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

16.1.2.2.5 “General Configuration” > “Home Dir On SD Card” Submenu

In this submenu, define if the home directory for the runtime system should be moved to the memory card.

Table 150: “PLC Runtime” > “General Configuration” > “Home Dir On SD Card” Submenu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. Enable	The home directory is moved to the memory card.
2. Disable	The home directory is stored in the internal memory.



Note

Insert a memory card before switching the home directory!

When moving the home directory to the memory card, insert a memory card formatted to support file system. Only the first partition of a memory card can be accessed at /media/sd and can be used as the home directory.



Note

Perform a reset before switching the home directory!

Stop IEC-61131 applications in use before switching the home directory of the runtime system.

Restore the device to its initial state using the “Reset” function. Any boot project is deleted.

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

16.1.2.2.6 “PLC Runtime” > “WebVisu” Submenu

This submenu contains information and settings for the Web visualization.

Table 151: “PLC Runtime” > “WebVisu” Submenu

Menu Item	Explanation	
0. Back to …	Back to the higher-level menu	
1. e!RUNTIME Webserver State	The status of the ***e!****RUNTIME* Webserver is displayed.	
2. Default Webserver	Choose here whether the Web-based Management or web visualization of the runtime system should be displayed when only entering the IP address of the controller.	
	0. Back to …	Back to the higher-level menu
	1. Web-based Management	The Web-based Management is displayed.
	2. CODESYS WebVisu	The web visualization of the runtime system is displayed.

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

16.1.2.3 “Networking” Menu

This menu contains other submenus with settings for the network configuration.

Table 152: “Networking” Menu

Parameters	Explanation
0. Back to …	Back to the higher-level menu
1. Host/Domain Name	Opens a submenu with setting options for the general TCP/IP parameters
2. TCP/IP	Opens a submenu with TCP/IP settings for the ETHERNET interfaces
3. Ethernet	Opens a submenu with settings for the ETHERNET configuration

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

16.1.2.3.1 “Networking” > “Host/Domain Name” Submenu

This submenu contains the “Hostname” and “Domain Name” submenu with setting options for the general TCP/IP parameters.

Table 153: “Networking” > “Host/Domain Name” Submenu

Parameters	Explanation
0. Back to …	Back to the higher-level menu
1. Hostname	Opens a submenu with the hostname settings In addition to the menu item, the configured and current hostname are displayed.
2. Domain Name	Opens a submenu hostname settings In addition to the menu item, the configured and current domain name are displayed.

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

16.1.2.3.2 “Host/Domain Name” > “Hostname” Submenu

In this submenu, you can set the hostname of the controller.

Table 154: “Networking” > “Hostname” Submenu

Parameters	Explanation
Enter new Hostname	Enter here the hostname of the controller to be used if the network interface is changed to a static IP address or if no hostname is transmitted with a DHCP response.

Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

16.1.2.3.3 “Host/Domain Name” > “Domain Name” Submenu

In this submenu, you can set the domain name of the controller.

Table 155: “Networking” > “Host/Domain Name” > “Domain Name” Submenu

Parameters	Explanation
Enter new Domain Name	Enter the domain name. The default entry is “localdomain.lan”.

Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

16.1.2.3.4 “Networking” > “TCP/IP” Submenu

This submenu contains other submenus with the TCP/IP settings for the ETHERNET interfaces.

Table 156: “Networking” > “TCP/IP” Submenu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. IP Address	Opens a submenu with settings for the IP address(es)
2. Default Gateway	Opens a submenu with settings for the default gateway
3. DNS Server	Opens a submenu with settings for the DNS server(s)

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

16.1.2.3.5 “TCP/IP” > “IP Address” Submenu

This submenu contains other submenus with settings for the ETHERNET interfaces.

The submenu only appears if the controller is operated in “Separated” mode. If the controller is operated in “Switched” mode, then the “IP Address” > “X1” submenu is displayed directly.

Table 157: “Networking” > “IP Address” Submenu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. X1	Opens a submenu with settings for the X1 interface
2. X2	Opens a submenu with settings for the X2 interface

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

16.1.2.3.6 “IP Address” > “Xn“ Submenu

This submenu contains the settings for the selected interface.

Table 158: “Networking” > “TCP/IP” > “IP Address” Submenu > “Xn”

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. Type of IP Address Configuration	Select a static or dynamic IP address.	
	0. Back to …	Back to the higher-level menu
	1. Static IP	Static IP addressing When selecting static addressing, the IP address and subnet mask are then retrieved.
	2. DHCP	Dynamic IP addressing
	3. BootP	Dynamic IP addressing
2. IP Address	Enter here a static IP address.	
3. Subnet Mask	Enter the subnet mask.	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.
Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

16.1.2.3.7 “TCP/IP” > “Default Gateway” Submenu

This submenu contains other submenus with settings for the default gateway.

Table 159: “Networking” > “TCP/IP” > “Default Gateway” Submenu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. Default Gateway 1	Opens a submenu with settings for default gateway 1 In addition to the menu item, the current status of the gateway is displayed.
2. Default Gateway 2	Opens a submenu with settings for default gateway 2 In addition to the menu item, the current status of the gateway is displayed.

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

16.1.2.3.8 “Default Gateway” > “Default Gateway n” Submenu

This submenu contains the settings for the selected gateway.

Table 160: “Networking” > “TCP/IP” > “Default Gateway” > “Default Gateway n” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. State	Set here whether the selected default gateway is to be used.	
	0. Back to …	Back to the higher-level menu
	1. Disabled	The default gateway is not used.
	2. Enabled	The default gateway is used.
2. Gateway IP Address	Enter the address of the default gateway.	
3. Gateway Metric	Set here a number as the metric. The default value for the metric is 20, the lowest value is 0, the highest value is 4.294.967.295.	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.
Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

16.1.2.3.9 “TCP/IP” > “DNS Server” Submenu

This submenu contains the settings for the DNS server.

Table 161: “Networking” > “TCP/IP” > “DNS Server” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
n. DNS Server n	The addresses of the defined DNS servers are displayed. Other submenus are available for the server entered.	
	0. Back to …	Back to the higher-level menu
	1. Edit	You can change the selected DNS server address.
	2. Delete	You can delete the selected DNS server address.
(n+1). Add new DNS Server	Add additional DNS server addresses. You can enter 10 addresses.	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.
Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

16.1.2.3.10 “Networking” > “Ethernet” Submenu

This submenu contains other submenus with settings for the ETHERNET configuration.

Table 162: “Networking” > “Ethernet” Submenu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. Switch Configuration	Opens a submenu with settings for the Switch Configuration
2. Ethernet Ports	Opens a submenu with settings for the ETHERNET interfaces

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

16.1.2.3.11 “Ethernet” > “Switch Configuration” Submenu

This submenu contains the settings for the Switch configuration.

Table 163: “Networking” > “Ethernet” > “Switch Configuration” Submenu

Submenu	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. Network interfaces	Enable or disable the switch.	
	0. Back to …	Back to the higher-level menu
	1. Separated	Each interface is operated with its own IP address.
	2. Switched	Both interfaces are operated with one IP address.

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

16.1.2.3.12 “Ethernet” > “Ethernet Ports” Submenu

This submenu contains other submenus with settings for the ETHERNET interfaces.

Table 164: “Networking” > “Ethernet” > “Ethernet Ports” Submenu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. Interface X1	Opens a submenu with settings for the X1 interface
2. Interface X2	Opens a submenu with settings for the X2 interface

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

16.1.2.3.13 “Ethernet Ports” > “Interface Xn” Submenu

This submenu contains the settings for the selected ETHERNET interface.

Table 165: “Networking” > “Ethernet” > “Ethernet Ports” > “Interface Xn” Submenu

Submenu	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. Port	Set here whether the selected port is to be used.	
	0. Back to …	Back to the higher-level menu
	1. Disabled	The port is not used.
	2. Enabled	The port is used.
2. Autonegotiation	Set here whether the Autonegotiation function is enabled for the selected port.	
	0. Back to …	Back to the higher-level menu
	1. Disabled	Autonegotiation is disabled.
	2. Enabled	Autonegotiation is enabled.

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

16.1.2.4 “Firewall” Menu

This menu contains other submenus for the firewall functionality settings.

Table 166: “Firewall” Menu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. General Configuration	Opens a submenu with general firewall settings
2. MAC Address Filter	Opens a submenu with MAC address filter settings
3. User Filter	Opens a submenu with user filter settings

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

16.1.2.4.1 “Firewall” > “General Configuration” Submenu

This submenu contains the general settings for the firewall.

Table 167: “Firewall” > “General Configuration” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. Firewall enabled entirely	Enables/disables the complete functionality of the firewall.	
	0. Back to …	Back to the higher-level menu
	1. Enable	Firewall is enabled.
	2. Disable	Firewall is disabled.
2. ICMP echo broadcast protection	Enable or disable the “ICMP echo broadcast” protection.	
	0. Back to …	Back to the higher-level menu
	1. Enable	“ICMP echo broadcast” protection is enabled.
	2. Disable	“ICMP echo broadcast” protection is disabled.
3. Max UDP connections per second	You can specify the maximum number of UDP connections per second. “0” = “Disabled”	
4. Max TCP connections per second	You can specify the maximum number of TCP connections per second. “0” = “Disabled”	
5. Interface VPN	Opens a submenu with firewall settings on the IP level for the selected interface	
6. Interface WAN		
7. Interface X1		
8. Interface X2		

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.
Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

16.1.2.4.2 “General Configuration” > “Interface xxx” Submenu

This submenu contains the firewall settings on the IP level for the selected interface.

Table 168: “Firewall” > “General Configuration” > “Interface xxx” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. Interface state	Enable or disable the firewall for the selected interface.	
	0. Back to …	Back to the higher-level menu
	1. Open	The firewall for the selected interface is disabled.
	2. Filtered	The firewall for the selected interface is enabled.
2. ICMP Policy	Enable or disable the “ICMP echo” protection for the respective interface.	
	0. Back to …	Back to the higher-level menu
	1. Accept	The “ICMP echo” protection is disabled.
	2. Drop	The “ICMP echo” protection is enabled.
3. ICMP Limit	You can specify the maximum number of “ICMP pings” per second. “0” = “Disabled”	
4. ICMP Burst	You can specify the maximum number of “ICMP echo bursts” per second. “0” = “Disabled”	
5. Telnet	Enable or disable the firewall for the respective service. The services themselves must be enabled or disabled separately on the “Ports and Services” page.	
6. FTP		
7. FTPS		
8. HTTP		
9. HTTPS		
10. I/O-CHECK		
11. PLC Runtime		
12. PLC WebVisu – direct link (port 8080)		
13. SSH		
14. TFTP		
15. BootP/DHCP		
16. DNS		
17. Modbus TCP		
18. Modbus UDP		
19. SNMP		

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

16.1.2.4.3 “Firewall” > “MAC Address Filter” Submenu

This submenu contains the settings for the MAC address filter.

Table 169: “Firewall” > “MAC Address Filter” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. Global MAC address filter state	Enable or disable the global MAC address filter.	
	0. Back to …	Back to the higher-level menu
	1. Filtered	The global MAC address filter is enabled.
	2. Open	The global MAC address filter is disabled.
2. MAC address filter whitelist	Opens a submenu to edit the MAC address filter whitelist	
3. MAC address filter state X1	Enable or disable the MAC address filter for the X1 interface.	
	0. Back to …	Back to the higher-level menu
	1. Open	The MAC address filter for the X1 interface is disabled.
	2. Filtered	The MAC address filter for the X1 interface is enabled.
4. MAC address filter state X2	Enable or disable the MAC address filter for the X2 interface.	
	0. Back to …	Back to the higher-level menu
	1. Open	The MAC address filter for the X2 interface is disabled.
	2. Filtered	The MAC address filter for the X2 interface is enabled.

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

16.1.2.4.4 “MAC Address Filter” > “MAC address filter whitelist” Submenu

This submenu displays all available filter entries.

Table 170: “Firewall” > “MAC Address Filter” > “MAC address filter whitelist” Submenu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. Add new	Opens a submenu to add a new filter entry You can enter 10 filters.
2. Previous page	Displays the previous page of the list (if more than one page is filled)
3. Next Page	Displays the next page of the list (if more than one page is filled)
(n + 3.) No (n):	Opens a submenu to edit an existing filter entry

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

16.1.2.4.5 “MAC address filter whitelist” > “Add new / No (n)” Submenu

In this submenu, you can create, change or delete filter entries.

Table 171: “Firewall” > “MAC Address Filter” > “MAC address filter whitelist” > “Add new / No (n)” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. MAC address	Enter the MAC address.	
2. MAC mask	Enter the MAC mask.	
3. Filter state	Enable or disable the filter.	
	0. Back to …	Back to the higher-level menu
	1. on	The filter is enabled.
	2. off	The filter is disabled.
4. accept	To apply the changes for the selected filter entry, choose this menu item.	
5. delete	To delete the selected filter entry, choose this menu item.	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.
Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

16.1.2.4.6 “Firewall” > “User Filter” Submenu

This submenu displays all available filter entries.

Table 172: “Firewall” > “User Filter” Submenu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. Add new	Opens a submenu to add a new filter entry
2. Previous page	Displays the previous page of the list (if more than one page is filled)
3. Next Page	Displays the next page of the list (if more than one page is filled)
(n + 3.) No (n):	Opens a submenu to edit an existing filter entry

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

16.1.2.4.7 “User Filter” > “Add New / No (n)” Submenu

In this submenu, you can create, change or delete filter entries.

Table 173: “Firewall” > “User Filter” > “Add New / No (n)” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. Policy	Select here whether the network devices is to be allowed or excluded by the filter.	
	0. Back to …	Back to the higher-level menu
	1. Allow	The network device is permitted.
	2. Drop	The network device is excluded.
2. Source IP address	Enter the source IP address.	
3. Source netmask	Enter the source network mask.	
4. Source port	Enter the source port number.	
5. Destination IP address	Enter the destination IP address.	
6. Destination netmask	Enter here the destination netmask.	
7. destination port	Enter the destination port number.	
8. protocol	Select the permitted protocols.	
	0. Back to …	Back to the higher-level menu
	1. tcp	The TCP protocol is permitted.
	2. udp	The UDP protocol is permitted.
	3. tcp & udp	Both protocols are permitted.
9. interface	Select the permitted interfaces.	
	0. Back to …	Back to the higher-level menu
	1. all	All interfaces are permitted.
	2. VPN	The VPN interface is permitted.
	3. WAN	The WAN interface is permitted.
	4. X1	The X1 interface is permitted.
	5. X2	The X2 interface is permitted.
10. state	Enable or disable the filter.	
	0. Back to …	Back to the higher-level menu
	1. on	The filter is enabled.
	2. off	The filter is disabled.
11. accept	To apply the changes for the selected filter entry, choose this menu item.	
12. delete	To delete the selected filter entry, choose this menu item.	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.
Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

16.1.2.5 “Clock” Menu

This menu contains other submenus for the date and time settings.

Table 174: “Clock” Menu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. Date on device (local)	Set date.	
2. Time on device (local)	Set local time.	
3. Time on device (UTC)	Set GMT time.	
4. Clock Display Mode	Select the display format for the time.	
	0. Back to …	Back to the higher-level menu
	1. 24 hours	The time is displayed in 24-hour format.
	2. 12 hours	The time is displayed in 12-hour format.
5. Timezone	Specify the appropriate time zone for your location. Basic setting:	
	0. Back to …	Back to the higher-level menu
	1. AST/ADT	“Atlantic Standard Time,” Halifax
	2. EST/EDT	“Eastern Standard Time,” New York, Toronto
	3. CST/CDT	“Central Standard Time,” Chicago, Winnipeg
	4. MST/ MDT	“Mountain Standard Time,” Denver, Edmonton
	5. PST/PDT	“Pacific Standard Time”, Los Angeles, Whitehouse
	6. GMT/BST	Greenwich Mean Time,“ GB, P, IRL, IS, …
	7. CET/ CEST	“Central European Time,” B, DK, D, F, I, CRO, NL, …
	8. EET/ EEST	“East European Time,” BUL, FI, GR, TR, …
	9. CST	“China Standard Time”
	10. JST	“Japan/Korea Standard Time”
6. TZ String	Enter the name of your time zone or country and town if the time zone is not available for selection using the “Timezone” parameter.	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.
Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

16.1.2.6 “Administration” Menu

This menu contains settings for controller administration.

Table 175: “Administration” Menu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. Users	Opens a submenu with settings for the user passwords	
2. Create Image	Opens a submenu for creating a bootable image	
3. Reboot Controller	Restart the controller following a security challenge.	
	0. Back to …	Back to the higher-level menu
	1. Reboot	Restarts the controller

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

16.1.2.6.1 “Administration” > “Users” Submenu

This submenu contains settings for the user passwords.

Table 176: “Administration” > “Users” Submenu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. user	Enter a new password for the “user” user.
2. admin	Enter a new password for the “admin” user.

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.
Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

16.1.2.6.2 “Administration” > “Create Image” Submenu

This submenu contains the selection for creating the image.

In addition to the menu item for the enabled storage medium, the current status is displayed.

Table 177: “Administration” > “Create Image” Submenu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. SD Card	To create an image on the memory card, select this menu item. Enter the reserved memory size in another step. This menu item only appears if the memory card is inserted.
2. Internal Flash	To create an image on the internal memory, select this menu item.

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.
Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

16.1.2.7 “Package Server” Menu

This menu contains other submenus with functions for firmware backup and restore, as well as information and setting options for the current system partition.

Table 178: “Package Server” Menu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. Firmware Backup	Opens a submenu with functions for the firmware backup
2. Firmware Restore	Opens a submenu with functions for the firmware restore
3. System Partition	Opens a submenu with information and setting options for the current system partition

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

16.1.2.7.1 “Package Server” > “Firmware Backup” Submenu

This submenu contains a selection option for the data to be saved.

The submenu only appears if a memory card is inserted that does not contain a bootable system. Otherwise, a message is displayed.

Table 179: “Package Server” > “Firmware Backup” Menu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. All	All data is saved.
2. PLC Runtime project	The PLC runtime project is saved.
3. Settings	The controller settings are saved.
4. System	The controller operating system is saved.

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

You are taken to the following submenu after making the selection.

16.1.2.7.2 “Firmware Backup” > “Auto Update Feature” Submenu

This submenu contains a setting option for the Auto Update function.

The submenu only appears if the data for the firmware backup has been selected.

Table 180: “Package Server” > “Firmware Backup” > “Auto Update Feature” Menu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. No	The Auto Update function is OFF for the selected data.
2. Yes	The Auto Update function is ON for the selected data.

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

You are taken to the following submenu after making the selection.

16.1.2.7.3 “Firmware Backup” > “Destination” Submenu

This submenu contains a selection option for the backup destination drive.

Table 181: “Package Server” > “Firmware Backup” > “Auto Update Feature” Menu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. SD Card	The selected data is copied to the memory card.

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

The copy progress is displayed during the backup process.

16.1.2.7.4 “Package Server” > “Firmware Restore” Submenu

This submenu contains a selection option for the restore source drive.

In addition to the enabled partition, the current status is displayed.

Table 182: “Package Server” > “Firmware Restore” Menu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. SD Card	The data is copied from the memory card.
2. Internal Flash	The data is copied from the internal memory.

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

You are taken to the following submenu after making the selection.

16.1.2.7.5 “Firmware Restore” > “Select Package” Submenu

This submenu contains a selection option for the data to be restored.

Table 183: “Package Server” > “Firmware Restore” > “Select Package” Menu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. PLC Runtime project	The PLC runtime project is loaded.
2. Settings	The controller settings are loaded.
3. System	The controller operating system is loaded.
4. System + Setting	The controller operating system and settings are loaded.
5. All	All data is loaded.

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

The copy progress is displayed during the restore process.

16.1.2.7.6 “Package Server” > “System Partition” Submenu

This submenu contains information and setting options for the current system partition.

Table 184: “Package Server” > “System Partition” Submenu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. Current active partition	The partition currently in use is displayed.
2. Set inactive NAND partition active	Select this menu item to start the system from a different partition at the next controller reboot.

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

16.1.2.8 “Mass Storage” Menu

This menu contains information on the internal flash memory and, if inserted, on the external memory card.

In addition to the menu item, the status is displayed for the enabled partition.

Table 185: “Mass Storage” Menu

Parameters	Explanation
0. Back to …	Back to the higher-level menu
1. SD Card	Opens a submenu with information on the memory card and its formatting This menu item only appears if a memory card is inserted in the controller.
2. Internal Flash	Opens a submenu with information on the internal flash memory

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

16.1.2.8.1 “Mass Storage” > “SD Card” Submenu

This submenu contains information on the external memory card and its formatting.

This submenu only appears if a memory card is inserted in the controller.

Table 186: “Mass Storage” > “SD Card” Menu

Parameters	Explanation
0. Back to …	Back to the higher-level menu
1. Show information	Displays information on the memory card
2. FAT format medium	To format the memory card in FAT format, select this menu item. Then specify a volume name.

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.
Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

16.1.2.9 “Software Uploads” Menu

This menu contains choices and settings for the device update.

You can select fieldbus software, program licenses and update scripts, for example, for transfer from a PC to the controller.
You can also enable transmitted packages or delete from the controller.

16.1.2.10 “Ports and Services” Menu

This submenu contains other submenus with settings for the respective services.

Table 187: “Ports and Services” Menu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. Telnet	Opens a submenu with settings for the Telnet service
2. FTP	Opens a submenu with settings for the FTP service
3. FTPS	Opens a submenu with settings for the FTPS service
4. HTTP	Opens a submenu with settings for the HTTP service
5. HTTPS	Opens a submenu with settings for the HTTPS service
6. NTP	Opens a submenu with settings for the NTP service
7. SSH	Opens a submenu with settings for the SSH server
8. TFTP	Opens a submenu with settings for the TFTP server
9. DHCPD	Opens a submenu with settings for the DHCPD service
10. DNS	Opens a submenu with settings for the DNS service
11. IOCHECK PORT	Opens a submenu with settings for the WAGO-I/O-CHECK port
12. Modbus TCP	Opens a submenu with settings for the Modbus TCP service
13. Modbus UDP	Opens a submenu with settings for the Modbus UDP service
14. OPC UA	Opens a submenu with settings for the OPC UA service
15. PLC Runtime Services	Opens a submenu with settings for the PLC runtime system services

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

16.1.2.10.1 “Ports and Services” > “Telnet” Submenu

This submenu contains the settings for the Telnet service.

Table 188: “Ports and Services” > “Telnet” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. State	Enable/disable the Telnet service.	
	0. Back to …	Back to the higher-level menu
	1. Enable	The Telnet service is enabled.
	2. Disable	The Telnet service is disabled.
2. Firewall status	Opens a submenu with firewall settings for the this service for the interfaces	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

16.1.2.10.2 “Ports and Services” > “FTP” Submenu

This submenu contains the settings for the FTP service.

Table 189: “Ports and Services” > “FTP” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. State	Enable/disable the FTP service.	
	0. Back to …	Back to the higher-level menu
	1. Enable	The FTP service is enabled.
	2. Disable	The FTP service is disabled.
2. Firewall status	Opens a submenu with firewall settings for the this service for the interfaces	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

16.1.2.10.3 “Ports and Services” > “FTPS” Submenu

This submenu contains the settings for the FTPS service.

Table 190: “Ports and Services” > “FTPS” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. State	Enable/disable the FTPS service.	
	0. Back to …	Back to the higher-level menu
	1. Enable	The FTPS service is enabled.
	2. Disable	The FTPS service is disabled.
2. Firewall status	Opens a submenu with firewall settings for the this service for the interfaces	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

16.1.2.10.4 “Ports and Services” > “HTTP” Submenu

This submenu contains the settings for the HTTP service.

Table 191: “Ports and Services” > “HTTP” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. State	Enable/disable the HTTP service.	
	0. Back to …	Back to the higher-level menu
	1. Enable	The HTTP service is enabled.
	2. Disable	The HTTP service is disabled.
2. Firewall status	Opens a submenu with firewall settings for the this service for the interfaces	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

16.1.2.10.5 “Ports and Services” > “HTTPS” Submenu

This submenu contains the settings for the HTTPS service.

Table 192: “Ports and Services” > “HTTPS” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. State	Enable/disable the HTTPS service.	
	0. Back to …	Back to the higher-level menu
	1. Enable	The HTTPS service is enabled.
	2. Disable	The HTTPS service is disabled.
2. Firewall status	Opens a submenu with firewall settings for the this service for the interfaces	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

16.1.2.10.6 “Ports and Services” > “NTP” Submenu

This submenu contains the settings for the NTP service.

Table 193: “Ports and Services” > “NTP” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. State	Enable/disable the NTP service.	
	0. Back to …	Back to the higher-level menu
	1. Enable	The NTP service is enabled.
	2. Disable	The NTP service is disabled.
2. Port	Enter the port number of the NTP server.	
3. Time Server 1	Enter here the IP addresses of up to 4 time servers. Time server No. 1 is requested first of all. If no data can be accessed via time server No. 1, time server No. 2 is requested.	
4. Time Server 2		
5. Time Server 3		
6. Time Server 4		
7. Update Time	Specify here the update interval of the time server.	
8. Issue immediate update	To update the time immediately, irrespective of the update interval, select this menu item.	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.
Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

16.1.2.10.7 “Ports and Services” > “SSH” Submenu

This submenu contains the settings for the SSH service.

Table 194: “Ports and Services” > “SSH” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. State	You can enable/disable the SSH server.	
	0. Back to …	Back to the higher-level menu
	1. Enable	The SSH server is enabled.
	2. Disable	The SSH server is disabled.
2. Port	Enter the port number.	
3. Allow root login	You can enable or inhibit root access.	
	0. Back to …	Back to the higher-level menu
	1. Enable	Root access is permitted.
	2. Disable	Root access is not permitted.
4. Allow password login	Enable or disable the password query function.	
	0. Back to …	Back to the higher-level menu
	1. Enable	Password query is enabled.
	2. Disable	Password query is disabled.
5. Status of firewalling	Opens a submenu with firewall settings for the this service for the interfaces	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

16.1.2.10.8 “Ports and Services” > “TFTP” Submenu

This submenu contains the settings for the TFTP service.

Table 195: “Ports and Services” > “TFTP” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. State	Enable or disable the TFTP server.	
	0. Back to …	Back to the higher-level menu
	1. Enable	The TFTP server is enabled.
	2. Disable	The TFTP server is disabled.
2. Transfer Directory	Specify here the path for downloading the server directory.	
3. Status of firewalling	Opens a submenu with firewall settings for the this service for the interfaces	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.
Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

16.1.2.10.9 “Ports and Services” > “DHCPD” Submenu

This submenu contains the settings for the DHCPD service.

Table 196: “Ports and Services” > “DHCPD” Submenu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. DHCPD firewalling	Opens a submenu with firewall settings for the this service for the interfaces
2. X1	Opens a submenu with the DHCPD settings for the selected interface
3. X2	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

16.1.2.10.10 “DHCPD” > “Xn” Submenu

This submenu contains the settings for the DHCPD service for the selected interface.

Table 197: “Ports and Services” > “DHCPD” > “Xn” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. State	Enable/disable the DHCPD service for the Xn interface.	
	0. Back to …	Back to the higher-level menu
	1. Enable	The DHCPD service is enabled.
	2. Disable	The DHCPD service is disabled.
2. Range	Enter a range of available IP addresses.	
3. Lease Time (min)	Specify the lease time here in seconds. 120 seconds are entered by default.	
4. Add static hostname	Enter a new static assignment of MAC ID to IP address, e.g., “01:02:03:04:05:06=192.168.1.20” or “hostname=192.168.1.20”. You can enter 10 assignments.	
(5 + n). Static Host (n)	This displays the static assignments.	
	0. Back to …	Back to the higher-level menu
	1. Edit	Opens a submenu to change the selected assignment
	2. Delete	Deletes the selected assignment

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.
Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

16.1.2.10.11 “Ports and Services” > “DNS” Submenu

This submenu contains the settings for the DNS service.

Table 198: “Ports and Services” > “DNS” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. State	Enable/disable the DNS service.	
	0. Back to …	Back to the higher-level menu
	1. Enable	The DNS service is enabled.
	2. Disable	The DNS service is disabled.
2. Mode	Select the operating mode of the DNS server.	
	0. Back to …	Back to the higher-level menu
	1. Proxy	The requests are buffered to optimize throughput.
	2. Relay	All requests are routed directly.
3. Firewall status	Opens a submenu with firewall settings for the this service for the interfaces	
4. Add static hostname	Enter a new static assignment of IP address to hostname, e.g., “192.168.1.20:hostname”. You can enter 10 assignments.	
(5 + n). Static Host (n)	This displays the hostnames for IP addresses.	
	0. Back to …	Back to the higher-level menu
	1. Edit	Opens a submenu to change the selected assignment
	2. Delete	Deletes the selected assignment

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.
Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

16.1.2.10.12 “Ports and Services” > “IOCHECK PORT” Submenu

This submenu contains settings for the WAGO-I/O-*CHECK* port.

Table 199: “Ports and Services” > “IOCHECK PORT” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. State	Enable/disable the WAGO-I/O-*CHECK* port.	
	0. Back to …	Back to the higher-level menu
	1. Enable	The WAGO-I/O-*CHECK* port is enabled.
	2. Disable	The WAGO-I/O-*CHECK* port is disabled.
2. Firewall status	Opens a submenu with firewall settings for the this service for the interfaces	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

16.1.2.10.13 “Ports and Services” > “Modbus TCP” Submenu

This submenu contains the settings for the Modbus TCP service.

Table 200: “Ports and Services” > “Modbus TCP” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. State	Disable or enable the Modbus/TCP service.	
	0. Back to …	Back to the higher-level menu
	1. Enable	The Modbus TCP service is enabled.
	2. Disable	The Modbus TCP service is disabled.
2. Firewall status	Opens a submenu with firewall settings for the this service for the interfaces	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

16.1.2.10.14 “Ports and Services” > “Modbus UDP” Submenu

This submenu contains the settings for the Modbus UDP service.

Table 201: “Ports and Services” > “Modbus UDP” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. State	Disable/enable the Modbus UDP service.	
	0. Back to …	Back to the higher-level menu
	1. Enable	The Modbus UDP service is enabled.
	2. Disable	The Modbus UDP service is disabled.
2. Firewall status	Opens a submenu with firewall settings for the this service for the interfaces	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

16.1.2.10.15 “Ports and Services” > “OPC UA” Submenu

This submenu contains the settings for the OPC UA service.

Table 202: “Ports and Services” > “OPC UA” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. State	Disable/enable the OPC UA service.	
	0. Back to …	Back to the higher-level menu
	1. Enable	The OPC UA service is enabled.
	2. Disable	The OPC UA service is disabled.
2. Firewall status	Opens a submenu with firewall settings for the this service for the interfaces	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

16.1.2.10.16 “…” > “Firewall Status” Submenu

This submenu contains firewall settings for the selected service.

Table 203: “Ports and Services” > “Firewall Status” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. VPN	Enable or disable the firewall for the VPN interface and respective service.	
	0. Back to …	Back to the higher-level menu
	1. open	Data traffic via the VPN interface is permitted.
	2. close	Data traffic via the VPN interface is not permitted.
2. WAN	Enable or disable the firewall for the WAN interface and respective service.	
	0. Back to …	Back to the higher-level menu
	1. open	Data traffic via the WAN interface is permitted.
	2. close	Data traffic via the WAN interface is not permitted.
3. X1	Enable or disable the firewall for the X1 interface and respective service.	
	0. Back to …	Back to the higher-level menu
	1. open	Data traffic via the X1 interface is permitted.
	2. close	Data traffic via the X1 interface is not permitted.
4. X2	Enable or disable the firewall for the X2 interface and respective service.	
	0. Back to …	Back to the higher-level menu
	1. open	Data traffic via the X2 interface is permitted.
	2. close	Data traffic via the X2 interface is not permitted.

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

16.1.2.10.17 “Ports and Services” > “PLC Runtime Services” Submenu

This submenu contains the settings for the PLC runtime system services.

Table 204: “Ports and Services” > “PLC Runtime Services” Submenu

Menu Item	Explanation
0. Back to …	Back to the higher-level menu
1. General Configuration	Enter the password for port authentication.
2. e!RUNTIME	Opens a submenu with service settings for ***e!****RUNTIME*
3. Change CODESYS Runtime firewalling settings	Opens a submenu with firewall settings for the this service for the interfaces
4. Change CODESYS WebVisu firewalling settings	Opens a submenu with firewall settings for the this service for the interfaces

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.
Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

16.1.2.10.18 “PLC Runtime Services” > “e!RUNTIME” Submenu

This submenu contains the settings for the ***e!****RUNTIME* service.

Table 205: “Ports and Services” > “PLC Runtime Services” > “e!RUNTIME” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. Webserver enable/disable	Enable or disable the Webserver for the ***e!****RUNTIME* web visualization.	
	0. Back to …	Back to the higher-level menu
	1. Enable	The Webserver is enabled.
	2. Disable	The Webserver is disabled.
2. Port Authentication enable/disable	Enter here whether a login is required for connecting to the device.	
	0. Back to …	Back to the higher-level menu
	1. Enable	Authentication via login is required.
	2. Disable	Authentication is not required.

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

16.1.2.11 “SNMP” Menu

This menu contains other submenus with the SNMP settings.

Table 206: “SNMP” Menu

Parameters	Explanation
0. Back to …	Back to the higher-level menu
1. General SNMP Configuration	Opens a submenu with general SNMP settings
2. SNMP v1/v2c Manager Configuration	Opens a submenu with settings for the SNMP v1/v2c Manager
3. SNMP v1/v2c Trap Receiver Configuration	Opens a submenu with settings for the SNMP v1/v2c trap receivers
4. SNMP v3 Configuration	Opens a submenu with settings for the SNMP v3 configuration
5. SNMP firewalling	Opens a submenu with firewall settings for SNMP
6. Secure SNMP firewalling	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

16.1.2.11.1 “SNMP” > “General SNMP Configuration” Submenu

This submenu contains the general SNMP settings.

Table 207: “SNMP” > “General SNMP Configuration” Submenu

Parameters	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. SNMP status	Enable or disable the SNMP service.	
	0. Back to …	Back to the higher-level menu
	1. Enable	The SNMP service is enabled.
	2. Disable	The SNMP service is disabled.
2. Name of device	Enter here the device name (sysName).	
3. Description	Enter here the device description (sysDescription).	
4. Physical location	Enter here the location of the device (sysLocation).	
5. Contact	Enter here the email contact address (sysContact).	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.
Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

16.1.2.11.2 “SNMP” > “SNMP v1/v2c Manager Configuration” Submenu

This submenu contains the SNMP v1/v2c Manager settings.

Table 208: “SNMP” > “SNMP v1/v2c Manager Configuration” Submenu

Parameters	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. Protocol state	Enable or disable the SNMP v1/v2c protocol.	
	0. Back to …	Back to the higher-level menu
	1. Enable	The SNMP v1/v2c protocol is enabled.
	2. Disable	The SNMP v1/v2c protocol is disabled.
2. Local community name	Specify here the community name for the SNMP manager configuration (max. 32 characters, no spaces).	

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.
Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

16.1.2.11.3 “SNMP” > “SNMP v1/v2c Trap Receiver Configuration” Submenu

This submenu contains settings for the v1/v2c trap receivers.

Table 209: “SNMP” > “SNMP v1/v2c Trap Receiver Configuration” Submenu

Parameters	Explanation
0. Back to …	Back to the higher-level menu
(n). Trap Receiver (n)	Opens a submenu with information on the selected v1/v2c trap receiver to delete the trap receiver
(n + 1). Add new Trap Receiver	Opens a series of submenus to create a new v1/v2c trap receiver You can enter 10 trap receivers. The following entries/selections are possible: • IP address of the new trap receiver (management station) • Community name for the new trap receiver configuration (max. 32 characters, no spaces) • SNMP version via which the traps are sent (v1/v2c)

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.
Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

16.1.2.11.4 “SNMP” > “SNMP v3 Configuration” Submenu

This submenu contains settings for SNMP v3.

Table 210: “SNMP” > “SNMP v3 Configuration” Submenu

Parameters	Explanation
0. Back to …	Back to the higher-level menu
(n). Username	Opens a submenu with information on the selected v3 user and to delete the user
(n + 1). Add new v3 User	Opens a series of submenus to create a new v3 user You can enter 10 users. The following entries/selections are possible: • Authentication name (The name can have a min. 8 and max. 32 characters and may contain lower case letters (a … z), upper case letters (A … Z), numbers (0 … 9), special characters !()*~'.-_ but no spaces.) • Authentication type (None/MD5/SHA) • Authentication key (The key can have a min. 8 and max. 32 characters and may contain lower case letters (a … z), upper case letters (A … Z), numbers (0 … 9), special characters !()*~'.-_ but no spaces.) • Privacy type (None/DES/AES) • Privacy key (The key can have a min. 8 and max. 32 characters and may contain lower case letters (a … z), upper case letters (A … Z), numbers (0 … 9), special characters !()*~'.-_ but no spaces.) • IP address for a trap receiver for v3 traps

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.
Click **[<OK>]** to apply the entry.
Click **[<Abort>]** to discard the entry.

16.1.2.11.5 “SNMP” > “(Secure)SNMP firewalling” Submenu

These submenus contain the SNMP firewall settings.

Table 211: “SNMP” > “(Secure)SNMP firewalling” Submenu

Menu Item	Submenu Item / Explanation	
0. Back to …	Back to the higher-level menu	
1. VPN	Enable or disable the firewall for the VPN interface and respective service.	
	0. Back to …	Back to the higher-level menu
	1. open	Data traffic via the VPN interface is permitted.
	2. close	Data traffic via the VPN interface is not permitted.
2. WAN	Enable or disable the firewall for the WAN interface and respective service.	
	0. Back to …	Back to the higher-level menu
	1. open	Data traffic via the WAN interface is permitted.
	2. close	Data traffic via the WAN interface is not permitted.
3. X1	Enable or disable the firewall for the X1 interface and respective service.	
	0. Back to …	Back to the higher-level menu
	1. open	Data traffic via the X1 interface is permitted.
	2. close	Data traffic via the X1 interface is not permitted.
4. X2	Enable or disable the firewall for the X2 interface and respective service.	
	0. Back to …	Back to the higher-level menu
	1. open	Data traffic via the X2 interface is permitted.
	2. close	Data traffic via the X2 interface is not permitted.

To make a selection, choose the appropriate menu item.
To return to the higher-level menu, press **[Q]**.

16.2 Process Data Architecture

The process image for the I/O modules on the local bus is built up word-by-word in the controller (with word alignment). The internal mapping method for data greater than one byte conforms to Intel formats.

The following section describes the representation for WAGO-I/O SYSTEM 750 (750 and 753 Series) I/O modules in the process image, as well as the configuration of the process values.

NOTICE

Equipment damage due to incorrect address!

To prevent any damage to the device in the field you must always take the process data for all previous byte or bit-oriented I/O modules into account when addressing an I/O module at any position in the fieldbus node.



Note

No direct access from fieldbus to the process image for I/O modules!

Any data that is required from the I/O module process image must be explicitly mapped in the CODESYS program to the data in the fieldbus process image and vice versa! Direct access is not possible!

16.2.1 Digital Input Modules

Digital input modules supply one bit of data per channel to specify the signal state for the corresponding channel. These bits are mapped into the Input Process Image.

Some digital modules have an additional diagnostic bit per channel in the Input Process Image. The diagnostic bit is used for detecting faults that occur (e.g., wire breaks and/or short circuits).

When analog input modules are also present in the node, the digital data is always appended after the analog data in the Input Process Image, grouped into bytes.

16.2.1.1 1 Channel Digital Input Module with Diagnostics

750-435

Table 212: 1 Channel Digital Input Module with Diagnostics

Input Process Image							
Bit 7	**Bit 6**	**Bit 5**	**Bit 4**	**Bit 3**	**Bit 2**	**Bit 1**	**Bit 0**
						Diagnostic bit S 1	Data bit DI 1

16.2.1.2 2 Channel Digital Input Modules

750-400, -401, -405, -406, -407, -410, -411, -412, -427, -438, (and all variations),
753-400, -401, -405, -406, -410, -411, -412, -427, -429

Table 213: 2 Channel Digital Input Modules

Input Process Image							
Bit 7	**Bit 6**	**Bit 5**	**Bit 4**	**Bit 3**	**Bit 2**	**Bit 1**	**Bit 0**
						Data bit DI 2 Channel 2	Data bit DI 1 Channel 1

16.2.1.3 2 Channel Digital Input Module with Diagnostics

750-419, -421, -424, -425,
753-421, -424, -425

Table 214: 2 Channel Digital Input Module with Diagnostics

Input Process Image							
Bit 7	**Bit 6**	**Bit 5**	**Bit 4**	**Bit 3**	**Bit 2**	**Bit 1**	**Bit 0**
				Diagnostic bit S 2 Channel 2	Diagnostic bit S 1 Channel 1	Data bit DI 2 Channel 2	Data bit DI 1 Channel 1

16.2.1.4 2 Channel Digital Input Module with Diagnostics and Output Process Data

750-418,
753-418

The digital input module supplies a diagnostic and acknowledge bit for each input channel. If a fault condition occurs, the diagnostic bit is set. After the fault condition is cleared, an acknowledge bit must be set to re-activate the input. The diagnostic data and input data bit is mapped in the Input Process Image, while the acknowledge bit is in the Output Process Image.

Table 215: 2 Channel Digital Input Module with Diagnostics and Output Process Data

Input Process Image							
Bit 7	**Bit 6**	**Bit 5**	**Bit 4**	**Bit 3**	**Bit 2**	**Bit 1**	**Bit 0**
				Diagnostic bit S 2 Channel 2	Diagnostic bit S 1 Channel 1	Data bit DI 2 Channel 2	Data bit DI 1 Channel 1

Output Process Image							
Bit 7	**Bit 6**	**Bit 5**	**Bit 4**	**Bit 3**	**Bit 2**	**Bit 1**	**Bit 0**
				Acknowledge-ment bit Q 2 Channel 2	Acknowledge-ment bit Q 1 Channel 1	0	0

16.2.1.5 4 Channel Digital Input Modules

750-402, -403, -408, -409, -414, -415, -422, -423, -428, -432, -433, -1420, -1421, -1422, -1423
753-402, -403, -408, -409, -415, -422, -423, -428, -432, -433, -440

Table 216: 4 Channel Digital Input Modules

Input Process Image							
Bit 7	**Bit 6**	**Bit 5**	**Bit 4**	**Bit 3**	**Bit 2**	**Bit 1**	**Bit 0**
				Data bit DI 4 Channel 4	Data bit DI 3 Channel 3	Data bit DI 2 Channel 2	Data bit DI 1 Channel 1

16.2.1.6 8 Channel Digital Input Modules

750-430, -431, -436, -437, -1415, -1416, -1417, -1418,
753-430, -431, -434, -436, -437

Table 217: 8 Channel Digital Input Modules

Input Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Data bit DI 8 Channel 8	Data bit DI 7 Channel 7	Data bit DI 6 Channel 6	Data bit DI 5 Channel 5	Data bit DI 4 Channel 4	Data bit DI 3 Channel 3	Data bit DI 2 Channel 2	Data bit DI 1 Channel 1

16.2.1.7 8 Channel Digital Input Module NAMUR with Diagnostics and Output Process Data

750-439

The digital input module NAMUR provides via one logical channel 2 byte for the input and output process image.

The signal state of NAMUR inputs DI1 … DI8 is transmitted to the fieldbus coupler/controller via input data byte D0.
The fault conditions are transmitted via input data byte D1.

The channels 1 … 8 are switched on or off via the output data byte D1.
The output data byte D0 is reserved and always has the value “0“.

Table 218: 8 Channel Digital Input Module NAMUR with Diagnostics and Output Process Data

Input Process Image							
Input byte D0							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Signal status DI 8 Channel 8	Signal status DI 7 Channel 7	Signal status DI 6 Channel 6	Signal status DI 5 Channel 5	Signal status DI 4 Channel 4	Signal status DI 3 Channel 3	Signal status DI 2 Channel 2	Signal status DI 1 Channel 1
Input byte D1							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Wire break /short circuit Data bit DI 8 Channel 8	Wire break /short circuit Data bit DI 7 Channel 7	Wire break /short circuit Data bit DI 6 Channel 6	Wire break /short circuit Data bit DI 5 Channel 5	Wire break /short circuit Data bit DI 4 Channel 4	Wire break /short circuit Data bit DI 3 Channel 3	Wire break /short circuit Data bit DI 2 Channel 2	Wire break /short circuit Data bit DI 1 Channel 1

Output Process Image							
Output byte D0							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	0	0	0	0	0	0	0
Output byte D1							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
DI Off 8 Channel 8 *)	DI Off 7 Channel 7 *)	DI Off 6 Channel 6 *)	DI Off 5 Channel 5 *)	DI Off 4 Channel 4 *)	DI Off 3 Channel 3 *)	DI Off 2 Channel 2 *)	DI Off 1 Channel 1 *)

*) 0: Channel ON
1: Channel OFF

16.2.1.8 8 Channel Digital Input Module PTC with Diagnostics and Output Process Data

750-1425

The digital input module PTC provides via one logical channel 2 byte for the input and output process image.

The signal state of PTC inputs DI1 … DI8 is transmitted to the fieldbus coupler/controller via input data byte D0.
The fault conditions are transmitted via input data byte D1.

The channels 1 … 8 are switched on or off via the output data byte D1.
The output data byte D0 is reserved and always has the value “0“.

Table 219: 8 Channel Digital Input Module PTC with Diagnostics and Output Process Data

Input Process Image							
Input Byte D0							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Signal status DI 8 Channel 8	Signal status DI 7 Channel 7	Signal status DI 6 Channel 6	Signal status DI 5 Channel 5	Signal status DI 4 Channel 4	Signal status DI 3 Channel 3	Signal status DI 2 Channel 2	Signal status DI 1 Channel 1
Input Byte D1							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Wire break /short circuit Data bit DI 8 Channel 8	Wire break /short circuit Data bit DI 7 Channel 7	Wire break /short circuit Data bit DI 6 Channel 6	Wire break /short circuit Data bit DI 5 Channel 5	Wire break /short circuit Data bit DI 4 Channel 4	Wire break /short circuit Data bit DI 3 Channel 3	Wire break /short circuit Data bit DI 2 Channel 2	Wire break /short circuit Data bit DI 1 Channel 1

Output Process Image							
Output Byte D0							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	0	0	0	0	0	0	0
Output Byte D1							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
DI Off 8 Channel 8 *)	DI Off 7 Channel 7 *)	DI Off 6 Channel 6 *)	DI Off 5 Channel 5 *)	DI Off 4 Channel 4 *)	DI Off 3 Channel 3 *)	DI Off 2 Channel 2 *)	DI Off 1 Channel 1 *)

*) 0: Channel ON
1: Channel OFF

16.2.2 16 Channel Digital Input Modules

750-1400, -1402, -1405, -1406, -1407

Table 220: 16 Channel Digital Input Modules

Input Process Image							
Input Byte D0							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Data bit DI 8 Channel 8	Data bit DI 7 Channel 7	Data bit DI 6 Channel 6	Data bit DI 5 Channel 5	Data bit DI 4 Channel 4	Data bit DI 3 Channel 3	Data bit DI 2 Channel 2	Data bit DI 1 Channel 1
Input Byte D1							
Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8
Data bit DI 16 Channel 16	Data bit DI 15 Channel 15	Data bit DI 14 Channel 4	Data bit DI 13 Channel 13	Data bit DI 12 Channel 12	Data bit DI 11 Channel 11	Data bit DI 10 Channel 10	Data bit DI 9 Channel 9

16.2.2.1 Digital Output Modules

Digital output modules use one bit of data per channel to control the output of the corresponding channel. These bits are mapped into the Output Process Image.

Some digital modules have an additional diagnostic bit per channel in the Input Process Image. The diagnostic bit is used for detecting faults that occur (e.g., wire breaks and/or short circuits). For modules with diagnostic bit is set, also the data bits have to be evaluated.

When analog output modules are also present in the node, the digital image data is always appended after the analog data in the Output Process Image, grouped into bytes.

16.2.2.2 1 Channel Digital Output Module with Input Process Data

750-523

The digital output module delivers 1 bit via a process value Bit in the output process image, which is illustrated in the input process image. This status image shows "manual mode".

Table 221: 1 Channel Digital Output Module with Input Process Data

Input Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
						not used	Status bit “Manual Operation“

Output Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
						not used	controls DO 1 Channel 1

16.2.2.3 2 Channel Digital Output Modules

750-501, -502, -509, -512, -513, -514, -517, -535, -538, (and all variations),
753-501, -502, -509, -512, -513, -514, -517

Table 222: 2 Channel Digital Output Modules

Output Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
						controls DO 2 Channel 2	controls DO 1 Channel 1

16.2.2.4 2 Channel Digital Input Modules with Diagnostics and Input Process Data

750-507 (-508), -522,
753-507

The digital output modules have a diagnostic bit for each output channel. When an output fault condition occurs (i.e., overload, short circuit, or broken wire), a diagnostic bit is set. The diagnostic data is mapped into the Input Process Image, while the output control bits are in the Output Process Image.

Table 223: 2 Channel Digital Input Modules with Diagnostics and Input Process Data

Input Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
						Diagnostic bit S 2 Channel 2	Diagnostic bit S 1 Channel 1

Output Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
						controls DO 2 Channel 2	controls DO 1 Channel 1

750-506,
753-506

The digital output module has 2-bits of diagnostic information for each output channel. The 2-bit diagnostic information can then be decoded to determine the exact fault condition of the module (i.e., overload, a short circuit, or a broken wire). The 4-bits of diagnostic data are mapped into the Input Process Image, while the output control bits are in the Output Process Image.

Table 224: 2 Channel Digital Input Modules with Diagnostics and Input Process Data 75x-506

Input Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
				Diagnostic bit S 3 Channel 2	Diagnostic bit S 2 Channel 2	Diagnostic bit S 1 Channel 1	Diagnostic bit S 0 Channel 1

Diagnostic bits S1/S0, S3/S2: = ‘00’ standard mode
Diagnostic bits S1/S0, S3/S2: = ‘01’ no connected load/short circuit against +24 V
Diagnostic bits S1/S0, S3/S2: = ‘10’ Short circuit to ground/overload

Output Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
				not used	not used	controls DO 2 Channel 2	controls DO 1 Channel 1

16.2.2.5 4 Channel Digital Output Modules

750-504, -515, -516, -519, -531,
753-504, -516, -531, -540

Table 225: 4 Channel Digital Output Modules

Output Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
				controls DO 4 Channel 4	controls DO 3 Channel 3	controls DO 2 Channel 2	controls DO 1 Channel 1

16.2.2.6 4 Channel Digital Output Modules with Diagnostics and Input Process Data

750-532, -539

The digital output modules have a diagnostic bit for each output channel. When an output fault condition occurs (i.e., overload, short circuit, or broken wire), a diagnostic bit is set. The diagnostic data is mapped into the Input Process Image, while the output control bits are in the Output Process Image.

Table 226: 4 Channel Digital Output Modules with Diagnostics and Input Process Data

Input Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
				Diagnostic bit S 4 Channel 4	Diagnostic bit S 3 Channel 3	Diagnostic bit S 2 Channel 2	Diagnostic bit S 1 Channel 1

Diagnostic bit S = ‘0’ no Error
Diagnostic bit S = ‘1’ overload, short circuit, or broken wire

Output Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
				controls DO 4 Channel 4	controls DO 3 Channel 3	controls DO 2 Channel 2	controls DO 1 Channel 1

16.2.2.7 8 Channel Digital Output Module

750-530, -536, -1515, -1516,
753-530, -534, 536

Table 227: 8 Channel Digital Output Module

Output Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
controls DO 8 Channel 8	controls DO 7 Channel 7	controls DO 6 Channel 6	controls DO 5 Channel 5	controls DO 4 Channel 4	controls DO 3 Channel 3	controls DO 2 Channel 2	controls DO 1 Channel 1

16.2.2.8 8 Channel Digital Output Modules with Diagnostics and Input Process Data

750-537,
753-537

The digital output modules have a diagnostic bit for each output channel. When an output fault condition occurs (i.e., overload, short circuit, or broken wire), a diagnostic bit is set. The diagnostic data is mapped into the Input Process Image, while the output control bits are in the Output Process Image.

Table 228: 8 Channel Digital Output Modules with Diagnostics and Input Process Data

Input Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Diagnostic bit S 8 Channel 8	Diagnostic bit S 7 Channel 7	Diagnostic bit S 6 Channel 6	Diagnostic bit S 5 Channel 5	Diagnostic bit S 4 Channel 4	Diagnostic bit S 3 Channel 3	Diagnostic bit S 2 Channel 2	Diagnostic bit S 1 Channel 1

Diagnostic bit S = ‘0’ no Error
Diagnostic bit S = ‘1’ overload, short circuit, or broken wire

Output Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
controls DO 8 Channel 8	controls DO 7 Channel 7	controls DO 6 Channel 6	controls DO 5 Channel 5	controls DO 4 Channel 4	controls DO 3 Channel 3	controls DO 2 Channel 2	controls DO 1 Channel 1

16.2.2.9 16 Channel Digital Output Modules

750-1500, -1501, -1504, -1505

Table 229: 16 Channel Digital Output Modules

Output Process Image							
Output Byte D0							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
controls DO 8 Channel 8	controls DO 7 Channel 7	controls DO 6 Channel 6	controls DO 5 Channel 5	controls DO 4 Channel 4	controls DO 3 Channel 3	controls DO 2 Channel 2	controls DO 1 Channel 1
Output Byte D1							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
controls DO 16 Channel 16	controls DO 15 Channel 15	controls DO 14 Channel 14	controls DO 13 Channel 13	controls DO 12 Channel 12	controls DO 11 Channel 11	controls DO 10 Channel 10	controls DO 9 Channel 9

16.2.2.10 8 Channel Digital Input/Output Modules

750-1502, -1506

Table 230: 8 Channel Digital Input/Output Modules

Input Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Data bit DI 8 Channel 8	Data bit DI 7 Channel 7	Data bit DI 6 Channel 6	Data bit DI 5 Channel 5	Data bit DI 4 Channel 4	Data bit DI 3 Channel 3	Data bit DI 2 Channel 2	Data bit DI 1 Channel 1

Output Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
controls DO 8 Channel 8	controls DO 7 Channel 7	controls DO 6 Channel 6	controls DO 5 Channel 5	controls DO 4 Channel 4	controls DO 3 Channel 3	controls DO 2 Channel 2	controls DO 1 Channel 1

16.2.3 Analog Input Modules

The analog input modules provide 16-bit measured data and 8 control/status bits per channel.

The controller only uses the 8 control/status bits internally for configuration/parameterization (e.g., via WAGO-I/O-*CHECK*).

Therefore, only the 16-bit measurement values for each channel are in Intel format and are mapped by word in the input process image for the controller.

When digital input modules are also present in the node, the analog input data is always mapped into the Input Process Image in front of the digital data.



Information

Information on the structure of control and status bytes
For detailed information on the structure of a particular I/O module's control/status bytes, please refer to that module's manual. Manuals for each module can be found on the Internet at www.wago.com.

16.2.3.1 1 Channel Analog Input Modules

750-491, (and all variations)

Table 231: 1 Channel Analog Input Modules

Input Process Image			
Offset	Byte Destination		Description
	High Byte	Low Byte	
0	D1	D0	Measured Value U_D
1	D3	D2	Measured Value U_{ref}

16.2.3.2 2 Channel Analog Input Modules

750-452, -454, -456, -461, -462, -464 (2-Channel Operation) -465, -466, -467, -469, -470, -472, -473, -474, -475, 476, -477, -478, -479, -480, -481, -483, -485, -487, -492, (and all variations),
753-452, -454, -456, -461, -465, -466, -467, -469, -472, -474, -475, -476, -477, -478, -479, -483, -492, (and all variations)

Table 232: 2 Channel Analog Input Modules

Input Process Image			
Offset	Byte Destination		Description
	High Byte	Low Byte	
0	D1	D0	Measured Value Channel 1
1	D3	D2	Measured Value Channel 2

16.2.3.3 2 Channel Analog Input Modules HART

750-482, -484, (and all variations),
753-482

The HART I/O module provides two different process images depending on the set operating mode.

For the pure analog values 4 mA ... 20 mA, the HART I/O module transmits 16 bit measured values per channel as an analog input module, which are mapped by word.

In operating mode "6 Byte Mailbox", the HART I/O module provides the fieldbus coupler / controller with a 12-byte input and output process image via a logical channel. For the control/status byte and the dummy byte, an acyclic channel (mailbox) for the process value communication is embedded in the process image, which occupies 6 bytes of data. This is followed by the measured values for channels 1 and 2.

HART commands are executed via the WAGO-IEC function blocks of the "WagoLibHart_0x.lib" library. The data is tunneled to the application via the mailbox and decoded by means of the library, so that the evaluation and processing takes place directly at the application level.

The operating mode is set using the WAGO-I / O-*CHECK* commissioning tool.

Table 233: 2-Channel Analog Input Modules HART

Input Process Image			
Offset	**Byte Destination**		**Description**
	High Byte	**Low Byte**	
0	D1	D0	Measured Value Channel 1
1	D3	D2	Measured Value Channel 2

Table 234:: 2 Channel Analog Input Modules HART + 6 bytes Mailbox

Input Process Image				
Offset	**Byte Destination**		**Description**	
	High Byte	**Low Byte**		
0	Internal Use	S0	Internal used	Status byte
1	MBX_RES	MBX_RES	Response data from mailbox	
2	MBX_RES	MBX_RES		
3	MBX_RES	MBX_RES		
4	D1	D0	Measured Value Channel 1	
5	D3	D2	Measured Value Channel 2	

Output Process Image			
Offset	**Byte Destination**		**Description**
	High Byte	**Low Byte**	
0	-	C0	Control byte
1	MBX_REQ	MBX_REQ	Request data from mailbox
2	MBX_REQ	MBX_REQ	
3	MBX_REQ	MBX_REQ	
4	-	-	Not used
5	-	-	

16.2.3.4 4 Channel Analog Input Modules

750-450, -453, -455, -457, -459, -460, -463, -464 (4-Channel Operation), -468, -471, -468, (and all variations),
753-453, -455, -457, -459

Table 235: 4 Channel Analog Input Modules

Input Process Image			
Offset	**Byte Destination**		**Description**
	High Byte	**Low Byte**	
0	D1	D0	Measured Value Channel 1
1	D3	D2	Measured Value Channel 2
2	D5	D4	Measured Value Channel 3
3	D7	D6	Measured Value Channel 4

16.2.3.5 8 Channel Analog Input Modules

750-451, 750-458, 750-496, 750-497

Table 236: 8 Channel Analog Input Modules

Input Process Image			
Offset	**Byte Destination**		**Description**
	High Byte	**Low Byte**	
0	D1	D0	Measured Value Channel 1
1	D3	D2	Measured Value Channel 2
2	D5	D4	Measured Value Channel 3
3	D7	D6	Measured Value Channel 4
4	D9	D8	Measured Value Channel 5
5	D11	D10	Measured Value Channel 6
6	D13	D12	Measured Value Channel 7
7	D15	D14	Measured Value Channel 8

16.2.3.6 3-Phase Power Measurement Module

750-493

The above Analog Input Modules have a total of 9 bytes of user data in both the Input and Output Process Image (6 bytes of data and 3 bytes of control/status). The following tables illustrate the Input and Output Process Image, which has a total of 6 words mapped into each image.
Word alignment is applied.

Table 237: 3-Phase Power Measurement Module

Input Process Image			
Offset	**Byte Destination**		**Description**
	High Byte	**Low Byte**	
0	-	S0	Status byte 0
1	D1	D0	Input data word 1
2	-	S1	Status byte 1
3	D3	D2	Input data word 2
4	-	S2	Status byte 2
5	D5	D4	Input data word 3

Output Process Image			
Offset	**Byte Destination**		**Description**
	High Byte	**Low Byte**	
0	-	C0	Control byte 0
1	D1	D0	Output data word 1
2	-	C1	Control byte 1
3	D3	D2	Output data word 2
4	-	C2	Control byte 2
5	D5	D4	Output data word 3

750-494, -495, (and all variations)

The 3-Phase Power Measurement Modules 750-494, -495, (and all variations) have a total of 24 bytes of user data in both the Input and Output Process Image (16 bytes of data and 8 bytes of control/status).

Table 238: 3-Phase Power Measurement Modules 750-494, -495, (and all variations)

Input Process Image			
Offset	**Byte Destination**		**Description**
	High Byte	**Low Byte**	
0	S1	S0	Status word
1	S3	S2	Extended status word 1
2	S5	S4	Extended status word 2
3	S7	S6	Extended status word 3
4	D1	D0	Process value 1
5	D3	D2	
6	D5	D4	Process value 2
7	D7	D6	
8	D9	D8	Process value 3
9	D11	D10	
10	D13	D12	Process value 4
11	D15	D14	

Output Process Image			
Offset	**Byte Destination**		**Description**
	High Byte	**Low Byte**	
0	S1	S0	Control word
1	S3	S2	Extended control word 1
2	S5	S4	Extended control word 2
3	S7	S6	Extended control word 3
4	-	-	-
5	-	-	
6	-	-	-
7	-	-	
8	-	-	-
9	-	-	
10	-	-	-
11	-	-	

16.2.4 Analog Output Modules

The analog output modules provide 16-bit output values and 8 control/status bits per channel.

The controller only uses the 8 control/status bits internally for configuration/parameterization (e.g., via WAGO-I/O-*CHECK*).

Therefore, only the 16-bit measurement values for each channel are in Intel format and are mapped by word in the output process image for the controller.

When digital output modules are also present in the node, the analog output data is always mapped into the Output Process Image in front of the digital data.



Information

Information on the structure of control and status bytes
For detailed information on the structure of a particular I/O module's control/status bytes, please refer to that module's manual. Manuals for each module can be found on the Internet at www.wago.com.

16.2.4.1 2 Channel Analog Output Modules

750-550, -552, -554, -556, -560, -562, 563, -585, -586, (and all variations),
753-550, -552, -554, -556

Table 239: 2 Channel Analog Output Modules

Output Process Image			
Offset	Byte Destination		Description
	High Byte	Low Byte	
0	D1	D0	Output Value Channel 1
1	D3	D2	Output Value Channel 2

16.2.4.2 4 Channel Analog Output Modules

750-553, -555, -557, -559,
753-553, -555, -557, -559

Table 240: 4 Channel Analog Output Modules

Output Process Image			
Offset	Byte Destination		Description
	High Byte	Low Byte	
0	D1	D0	Output Value Channel 1
1	D3	D2	Output Value Channel 2
2	D5	D4	Output Value Channel 3
3	D7	D6	Output Value Channel 4

16.2.5 Specialty Modules

WAGO has a host of Specialty I/O modules that perform various functions. With individual modules beside the data bytes also the control/status byte is mapped in the process image.

The control/status byte is required for the bidirectional data exchange of the module with the higher-ranking control system. The control byte is transmitted from the control system to the module and the status byte from the module to the control system.
This allows, for example, setting of a counter with the control byte or displaying of overshooting or undershooting of the range with the status byte.

The control/status byte always is in the process image in the Low byte.



Information

Information about the structure of the Control/Status byte
For detailed information about the structure of a particular module's control/status byte, please refer to that module's manual. Manuals for each module can be found on the Internet under: www.wago.com.

16.2.5.1 Counter Modules

750-404, (and all variations except of /000-005),
753-404, -404/000-003

The above Counter Modules have a total of 5 bytes of user data in both the Input and Output Process Image (4 bytes of counter data and 1 byte of control/status). The counter value is supplied as 32 bits. The following tables illustrate the Input and Output Process Image, which has a total of 3 words mapped into each image. Word alignment is applied.

Table 241: Counter Modules 750-404, (and all variations except of /000-005), 753-404, -404/000-003

Input Process Image			
Offset	Byte Designation		Description
	High Byte	Low Byte	
0	-	S	Status byte
1	D1	D0	Counter value
2	D3	D2	

Output Process Image			
Offset	Byte Designation		Description
	High Byte	Low Byte	
0	-	C	Control byte
1	D1	D0	Counter setting value
2	D3	D2	

750-404/000-005,
753-404/000-005

The above Counter Modules have a total of 5 bytes of user data in both the Input and Output Process Image (4 bytes of counter data and 1 byte of control/ status). The two counter values are supplied as 32 bits. The following tables illustrate the Input and Output Process Image, which has a total of 3 words mapped into each image. Word alignment is applied.

Table 242: Counter Modules 750-404/000-005, 753-404/000-005

Input Process Image			
Offset	**Byte Designation**		**Description**
	High Byte	**Low Byte**	
0	-	S	Status byte
1	D1	D0	Counter Value of Counter 1
2	D3	D2	Counter Value of Counter 2

Output Process Image			
Offset	**Byte Designation**		**Description**
	High Byte	**Low Byte**	
0	-	C	Control byte
1	D1	D0	Counter Setting Value of Counter 1
2	D3	D2	Counter Setting Value of Counter 2

750-633

The above Counter Module has a total of 5 bytes of user data in both the Input and Output Process Image (4 bytes of counter data and 1 byte of control/ status). The following tables illustrate the Input and Output Process Image, which has a total of 3 words mapped into each image. Word alignment is applied.
The meaning of the output data depends on the set operating mode:
1 Up counter with enable input
2 Up/down counter with U/D input
3 Frequency counter
4 Gate time counter

Table 243: Counter Modules 750-633

Input Process Image			
Offset	**Byte Designation**		**Description**
	High Byte	**Low Byte**	
0	-	S	Status byte
1	D1	D0	Counter Value
2	D3	D2	

Output Process Image			
Offset	**Byte Designation**		**Description**
	High Byte	**Low Byte**	
0	-	C	Control byte
1	D1	D0	Counter Setting Value [1,2)] watchdog time [3)] reserved [4)]
2	D3	D2	Counter Setting Value [1,2)] reserved [3)] reserved [4)]

[1,2)] Up counter with enable input, Up /down counter with U / D input
[3)] Frequency counter
[4)] Gate time counter

750-638,
753-638

The above Counter Modules have a total of 6 bytes of user data in both the Input and Output Process Image (4 bytes of counter data and 2 bytes of control/status). The two counter values are supplied as 16 bits. The following tables illustrate the Input and Output Process Image, which has a total of 4 words mapped into each image. Word alignment is applied.

Table 244: Counter Modules 750-638, 753-638

Input Process Image			
Offset	**Byte Designation**		**Description**
	High Byte	**Low Byte**	
0	-	S0	Status byte of Counter 1
1	D1	D0	Counter Value of Counter 1
2	-	S1	Status byte of Counter 2
3	D3	D2	Counter Value of Counter 2

Output Process Image			
Offset	Byte Designation		Description
	High Byte	Low Byte	
0	-	C0	Control byte of Counter 1
1	D1	D0	Counter Setting Value of Counter 1
2	-	C1	Control byte of Counter 2
3	D3	D2	Counter Setting Value of Counter 2

16.2.5.2 Pulse Width Modules

750-511, (and all variations),
753-511

The above Pulse Width modules have a total of 6 bytes of user data in both the Input and Output Process Image (4 bytes of channel data and 2 bytes of control/ status). The two channel values are supplied as 16 bits. Each channel has its own control/status byte. The following table illustrates the Input and Output Process Image, which has a total of 4 words mapped into each image. Word alignment is applied.

Table 245: Pulse Width Modules 750-511, /xxx-xxx, 753-511

Input and Output Process			
Offset	Byte Designation		Description
	High Byte	Low Byte	
0	-	C0/S0	Control/Status byte of Channel 1
1	D1	D0	Data Value of Channel 1
2	-	C1/S1	Control/Status byte of Channel 2
3	D3	D2	Data Value of Channel 2

16.2.5.3 Serial Interface Modules with Alternative Data Format

750-650, (and the variations /000-002, -004, -006, -009, -010, -011, -012, -013),
750-651, (and the variations /000-001, -002, -003),
750-653, (and the variations /000-002, -007),
753-650, -653

Note

The process image of the / 003-000-variants depends on the parameterized operating mode!
With the freely parameterizable variations /003 000 of the serial interface modules, the desired operating mode can be set. Dependent on it, the process image of these modules is then the same, as from the appropriate variation.

The above Serial Interface Modules with alternative data format have a total of 4 bytes of user data in both the Input and Output Process Image (3 bytes of serial data and 1 byte of control/status). The following table illustrates the Input and

Output Process Image, which have a total of 2 words mapped into each image. Word alignment is applied.

Table 246: Serial Interface Modules with Alternative Data Format

Input and Output Process Image				
Offset	**Byte Designation**		**Description**	
	High Byte	**Low Byte**		
0	D0	C/S	Data byte	Control/status byte
1	D2	D1	Data bytes	

16.2.5.4 Serial Interface Modules with Standard Data Format

750-650/000-001, -014, -015, -016,
750-651/000-001,
750-653/000-001, -006

The above Serial Interface Modules with Standard Data Format have a total of 6 bytes of user data in both the Input and Output Process Image (5 bytes of serial data and 1 byte of control/status). The following table illustrates the Input and Output Process Image, which have a total of 3 words mapped into each image. Word alignment is applied.

Table 247: Serial Interface Modules with Standard Data Format

Input and Output Process Image				
Offset	**Byte Designation**		**Description**	
	High Byte	**Low Byte**		
0	D0	C/S	Data byte	Control/status byte
1	D2	D1	Data bytes	
2	D4	D3		

16.2.5.5 Serial Interface Modules

750-652,
753-652

The size of the process image for the Serial Interface Module can be adjusted to 12, 24 or 48 bytes.
It consists of two status bytes (input) or control bytes (output) and the process data with a size of 6 to 46 bytes.

Thus, each Serial Interface Module uses between 8 and 48 bytes in the process image. The sizes of the input and output process images are always the same.

The process image sizes are set with the startup tool WAGO-I/O-*CHECK*.

Table 248: Serial Interface Modules 750-652, 753-652

Input and Output Process Image					
Process image size	**Offset**	**Byte Designation**		**Description**	
		High Byte	**Low Byte**		
8 bytes	0	C1/S1	C0/S0	Control/Status byte C1/S1	Control/Status byte C0/S0
	1	D1	D0	Prozess data (6-46 bytes)	
	2	D3	D2		
	3	D5	D4		
24 bytes*	4	D7	D6		
	…				
	11	D21	D20		
48 bytes	12	D23	D22		
	…				
	23	D45	D44		

*) Factory setting

16.2.5.6 Data Exchange Module

750-654, -654/000-001

The Data Exchange modules have a total of 4 bytes of user data in both the Input and Output Process Image. The following tables illustrate the Input and Output Process Image, which has a total of 2 words mapped into each image.
Word alignment is applied.

Table 249: Data Exchange Module 750-654, -654/000-001

Input and Output Process Image			
Offset	**Byte Designation**		**Description**
	High Byte	**Low Byte**	
0	D1	D0	Data bytes
1	D3	D2	

16.2.5.7 SSI Transmitter Interface Modules

750-630, and the variations /000-001, -002, -006, -008, -009, -011, -012, -013

Note

The process image of the / 003-000-variants depends on the parameterized operating mode!
The operating mode of the configurable /003-000 I/O module versions can be set. Based on the operating mode, the process image of these I/O modules is then the same as that of the respective version.

The above SSI Transmitter Interface modules have a total of 4 bytes of user data in the Input Process Image, which has 2 words mapped into the image.
Word alignment is applied.

Table 250: SSI Transmitter Interface Modules

Input Process Image			
Offset	**Byte Designation**		**Description**
	High Byte	**Low Byte**	
0	D1	D0	Data bytes
1	D3	D2	

750-630/000-004, -005, -007

In the input process image, SSI transmitter interface modules with status occupy 5 usable bytes, 4 data bytes, and 1 additional status byte. A total of 3 words are assigned in the process image via word alignment.

Table 251: SSI Transmitter Interface I/O Modules with an Alternative Data Format (/000-004, -005, -007)

Input Process Image				
Offset	**Byte Destination**		**Description**	
	High Byte	**High Byte**		
0	-	S	not used	Status byte
1	D1	D0	Data bytes	
2	D3	D2		

16.2.5.8 Incremental Encoder Interface Modules

Incremental Encoder Interface Modules

750-631/000-004, -010, -011

The above Incremental Encoder Interface modules have 5 bytes of input data and 3 bytes of output data. The following tables illustrate the Input and Output Process Image, which have 4 words into each image. Word alignment is applied.

Table 252: Incremental Encoder Interface Modules 750-631/000-004, --010, -011

Input Process Image				
Offset	**Byte Designation**		**Description**	
	High Byte	**Low Byte**		
0	-	S	not used	Status byte
1	D1	D0	Counter word	
2	-	-	not used	
3	D4	D3	Latch word	

Output Process Image				
Offset	**Byte Designation**		**Description**	
	High Byte	**Low Byte**		
0	-	C	not used	Control byte
1	D1	D0	Counter setting word	
2	-	-	not used	
3	-	-	not used	

750-634

The above Incremental Encoder Interface module has 5 bytes of input data (6 bytes in cycle duration measurement mode) and 3 bytes of output data. The following tables illustrate the Input and Output Process Image, which has 4 words mapped into each image. Word alignment is applied.

Table 253: Incremental Encoder Interface Modules 750-634

Input Process Image				
Offset	**Byte Designation**		**Description**	
	High Byte	**Low Byte**		
0	-	S	not used	Status byte
1	D1	D0	Counter word	
2	-	(D2) *)	not used	(Periodic time)
3	D4	D3	Latch word	

*) If cycle duration measurement mode is enabled in the control byte, the cycle duration is given as a 24-bit value that is stored in D2 together with D3/D4.

Output Process Image				
Offset	**Byte Designation**		**Description**	
	High Byte	**Low Byte**		
0	-	C	not used	Control byte
1	D1	D0	Counter setting word	
2	-	-	not used	
3	-	-		

750-637, (and all variations)

The above Incremental Encoder Interface Module has a total of 6 bytes of user data in both the Input and Output Process Image (4 bytes of encoder data and 2 bytes of control/status). The following table illustrates the Input and Output Process Image, which have 4 words mapped into each image. Word alignment is applied.

Table 254: Incremental Encoder Interface Modules 750-637, (and all variations)

Input and Output Process Image			
Offset	**Byte Designation**		**Description**
	High Byte	**Low Byte**	
0	-	C0/S0	Control/Status byte of Channel 1
1	D1	D0	Data Value of Channel 1
2	-	C1/S1	Control/Status byte of Channel 2
3	D3	D2	Data Value of Channel 2

Digital Pulse Interface module

750-635,
753-635

The above Digital Pulse Interface module has a total of 4 bytes of user data in both the Input and Output Process Image (3 bytes of module data and 1 byte of control/status). The following table illustrates the Input and Output Process Image, which have 2 words mapped into each image. Word alignment is applied.

Table 255: Digital Pulse Interface Modules 750-635, 753-635

Input and Output Process Image				
Offset	Byte Designation		Description	
	High Byte	Low Byte		
0	D0	C0/S0	Data byte	Control/status byte
1	D2	D1	Data bytes	

16.2.5.9 DC-Drive Controller

750-636, -636/000-700, -636/000-800

The DC-Drive Controller maps 6 bytes into both the input and output process image. The data sent and received are stored in up to 4 input and output bytes (D0 ... D3). Two control bytes (C0, C1) and two status bytes (S0/S1) are used to control the I/O module and the drive.

In addition to the position data in the input process image (D0 … D3), it is possible to display extended status information (S2 … S5). Then the three control bytes (C1 … C3) and status bytes (S1 … S3) are used to control the data flow.

Bit 3 of control byte C1 (C1.3) is used to switch between the process data and the extended status bytes in the input process image (Extended Info_ON). Bit 3 of status byte S1 (S1.3) is used to acknowledge the switching process.

Table 256: DC-Drive Controller 750-636, -636/000-700, -636/000-800

Input Process Image				
Offset	Byte Designation		Description	
	High Byte	Low Byte		
0	S1	S0	Status byte S1	Status byte S0
1	D1*) / S3**)	D0*) / S2**)	Actual position*) / Extended status byte S3**)	Actual position (LSB) / Extended status byte S2**)
2	D3*) / S5**)	D2*) / S4**)	Actual position (MSB) / Extended status byte S3**)	Actual position*) / Extended status byte S4**)

*) ExtendedInfo_ON = ‘0’.
**) ExtendedInfo_ON = ‘1’.

Output Process Image				
Offset	Byte Designation		Description	
	High Byte	Low Byte		
0	C1	C0	Control byte C1	Control byte C0
1	D1	D0	Setpoint position	Setpoint position (LSB)
2	D3	D2	Setpoint position (MSB)	Setpoint position

16.2.5.10 Stepper Controller

750-670, -671, -672

The Stepper controller provides the fieldbus coupler/controller 12 bytes input and output process image via 1 logical channel. The data to be sent and received are stored in up to 7 output bytes (D0 … D6) and 7 input bytes (D0 … D6), depending on the operating mode.

Output byte D0 and input byte D0 are reserved and have no function assigned.

One I/O module control and status byte (C0, S0) and 3 application control and status bytes (C1 ... C3, S1 ... S3) provide the control of the data flow.

Switching between the two process images is conducted through bit 5 in the control byte (C0 (C0.5). Activation of the mailbox is acknowledged by bit 5 of the status byte S0 (S0.5).

Table 257: Stepper Controller 750-670, -671, -672

Input and Output Process Image				
Offset	Byte Designation		Description	
	High Byte	Low Byte		
0	Reserviert	C0/S0	reserved	Control/Status byte C0/S0
1	D1	D0	Process data*) / Mailbox**)	
2	D3	D2		
3	D5	D4		
4	S3	D6	Control/Status byte C3/S3	Process data*) / reserved**)
5	C1/S1	C2/S2	Control/Status byte C1/S1	Control/Status byte C2/S2

*) Cyclic process image (Mailbox disabled)

**) Mailbox process image (Mailbox activated)

16.2.5.11 RTC Module

750-640

The RTC Module has a total of 6 bytes of user data in both the Input and Output Process Image (4 bytes of module data and 1 byte of control/status and 1 byte ID for command). The following table illustrates the Input and Output Process Image, which have 3 words mapped into each image. Word alignment is applied.

Table 258: RTC Module 750-640

Input and Output Process Image				
Offset	**Byte Designation**		**Description**	
	High Byte	**Low Byte**		
0	ID	C/S	Command byte	Control/status byte
1	D1	D0	Data bytes	
2	D3	D2		

16.2.5.12 DALI Multi-Master Module

753-647

The DALI Multi-Master module occupies a total of 24 bytes in the input and output range of the process image.

The DALI Multi-Master module can be operated in "Easy" mode (default) and "Full" mode. "Easy" mode is used to transmit simply binary signals for lighting control. Configuration or programming via DALI master module is unnecessary in "Easy" mode.

Changes to individual bits of the process image are converted directly into DALI commands for a pre-configured DALI network. 22 bytes of the 24-byte process image can be used directly for switching of electronic ballasts (ECG), groups or scenes in "Easy" mode. Switching commands are transmitted via DALI and group addresses, where each DALI and each group address is represented by a 2-bit pair.

In full mode, the 24 bytes of the process image are used to tunnel a protocol using a mailbox interface. The process image consists of 1 byte for control / status and 23 bytes for the acyclic data.

The structure of the process data is described in detail in the following tables.

Table 259: DALI Multi-Master Module 753-647 in the "Easy" Mode

Input Process Image				
Offset	**Byte Designation**		**Note**	
	High Byte	**Low Byte**		
0	-	S	res.	Status, activate broadcast Bit 0: 1-/2-button mode Bit 2: Broadcast status ON/OFF Bit 1,3-7: -
1	DA4…DA7	DA0…DA3	Bit pair for DALI address DA0: Bit 1: Bit set = ON Bit not set = OFF Bit 2: Bit set = Error Bit not set = No error Bit pairs DA1 … DA63 similar to DA0.	
2	DA12…DA15	DA8…DA11		
3	DA20…DA23	DA16…DA19		
4	DA28…DA31	DA24…DA27		
5	DA36…DA39	DA32…DA35		
6	DA44…DA47	DA40…DA43		
7	DA52…DA55	DA48…DA51		
8	DA60…DA63	DA56…DA59		
9	GA4…GA7	GA0…GA3	Bit pair for DALI group address GA0: Bit 1: Bit set = ON Bit not set = OFF Bit 2: Bit set = Error Bit not set = No error Bit pairs GA1 … GA15 similar to GA0.	
10	GA12…GA15	GA8…GA11		
11	-	-	Not used	

DA = DALI address
GA = Group address

Output Process Image				
Offset	**Byte Designation**		**Note**	
	High Byte	**Low Byte**		
0	-	C	res.	Bit 0: Broadcast ON Bit 1: Broadcast OFF Bit 2: (1 button operation): - short: Broadcast ON/OFF - long: Broadcast dimming brighter/darker Bit 2: (2 buttons operation): - short: Broadcast ON/OFF - long: Broadcast dimming brighter Bit 3: (1 button operation): Broadcast ON/OFF Bit 3: (2 buttons operation): - short: Broadcast ON/OFF - long: Broadcast dimming darker Bit 4: Watchdog toggling (starting from FW06 of the DALI Multi-Master) Bit 5…7: reserved
1	DA4…DA7	DA0…DA3	Bit pair for DALI address: Bit 1 (1 button operation): - short: DA switch ON/OFF - long: dimming brighter/darker Bit 1 (2 buttons operation): - short: DA switch ON - long: dimming brighter Bit 2 (1 button operation): DA switch ON/OFF Bit 2 (2 buttons operation): - short: DA switch OFF - long: dimming darker	
2	DA12…DA15	DA8…DA11		
3	DA20…DA23	DA16…DA19		
4	DA28…DA31	DA24…DA27		
5	DA36…DA39	DA32…DA35		
6	DA44…DA47	DA40…DA43		
7	DA52…DA55	DA48…DA51		
8	DA60…DA63	DA56…DA59		
9	GA4…GA7	GA0…GA3	Bit pair for DALI group address: Bit 1 (1 button operation): - short: GA switch ON/OFF - long: dimming brighter/darker Bit 1 (2 buttons operation): - short: GA switch ON - long: dimming brighter Bit 2 (1 button operation): GA switch ON/OFF Bit 2 (2 buttons operation): - short: GA switch OFF - long: dimming darker	
10	GA12…GA15	GA8…GA11		
11	Bit 8…15	Bit 0…7	Switch scene 0…15	

DA = DALI address
GA = Group address

Table 260: DALI Multi-Master Module 753-647 in the "Full" Mode

Input and Output Process Image				
Offset	**Byte Designation**		**Note**	
	High Byte	**Low Byte**		
0	MBX_C/S	C0/S0	Mailbox control/status byte	control/status byte
1	MBX1	MBX0	Mailbox	
2	MBX3	MBX2		
3	MBX5	MBX4		
4	MBX7	MBX6		
5	MBX9	MBX8		
6	MBX11	MBX10		
7	MBX13	MBX12		
8	MBX15	MBX14		
9	MBX17	MBX16		
10	MBX19	MBX18		
11	MBX21	MBX20		

16.2.5.13 LON® FTT Module

753-648

The process image of the LON® FTT module consists of a control/status byte and 23 bytes of bidirectional communication data that is processed by the WAGO-I/O-*PRO* function block "LON_01.lib". This function block is essential for the function of the LON® FTT module and provides a user interface on the control side.

Table 261: LON® FTT Module 753-648

Input and Output Process Image				
Offset	**Byte Designation**		**Note**	
	High Byte	**Low Byte**		
0	MBX_C/S	C0/S0	Mailbox control/status byte	control/status byte
1	MBX1	MBX0	Mailbox	
2	MBX3	MBX2		
3	MBX5	MBX4		
4	MBX7	MBX6		
5	MBX9	MBX8		
6	MBX11	MBX10		
7	MBX13	MBX12		
8	MBX15	MBX14		
9	MBX17	MBX16		
10	MBX19	MBX18		
11	MBX21	MBX20		

16.2.5.14 EnOcean Radio Receiver

750-642

The EnOcean radio receiver has a total of 4 bytes of user data in both the Input and Output Process Image (3 bytes of module data and 1 byte of control/status). The following tables illustrate the Input and Output Process Image, which have 2 words mapped into each image. Word alignment is applied.

Table 262: EnOcean Radio Receiver 750-642

Input Process Image				
Offset	**Byte Destination**		**Description**	
	High Byte	**Low Byte**		
0	D0	S	Data byte	Status byte
1	D2	D1	Data bytes	

Output Process Image				
Offset	**Byte Destination**		**Description**	
	High Byte	**Low Byte**		
0	-	C	not used	Control byte
1	-	-	not used	

16.2.5.15 MP Bus Master Module

750-643

The MP Bus Master Module has a total of 8 bytes of user data in both the Input and Output Process Image (6 bytes of module data and 2 bytes of control/status). The following table illustrates the Input and Output Process Image, which have 4 words mapped into each image. Word alignment is applied.

Table 263: MP Bus Master Module 750-643

Input and Output Process Image				
Offset	**Byte Destination**		**Description**	
	High Byte	**Low Byte**		
0	C1/S1	C0/S0	Extended Control/ Status byte	Control/status byte
1	D1	D0	Data bytes	
2	D3	D2		
3	D5	D4		

16.2.5.16 *Bluetooth*® RF-Transceiver

750-644

The size of the process image for the *Bluetooth*® module can be adjusted to 12, 24 or 48 bytes.
It consists of one control byte (input) or status byte (output); an empty byte; an overlay able mailbox with a size of 6, 12 or 18 bytes (mode 2); and the *Bluetooth*® process data with a size of 4 to 46 bytes.
Thus, each *Bluetooth*® module uses between 12 and 48 bytes in the process image. The sizes of the input and output process images are always the same.

The first byte contains the control/status byte; the second contains an empty byte.

Process data attach to this directly when the mailbox is hidden. When the mailbox is visible, the first 6, 12 or 18 bytes of process data are overlaid by the mailbox data, depending on their size. Bytes in the area behind the optionally visible mailbox contain basic process data. The internal structure of the *Bluetooth*® process data can be found in the documentation for the *Bluetooth*® 750-644 RF Transceiver.

The mailbox and the process image sizes are set with the startup tool WAGO-I/O-*CHECK*.

Table 264: *Bluetooth*® RF-Transceiver 750-644

Input and Output Process Image					
Process image size	**Offset**	**Byte Destination**		**Description**	
		High Byte	**Low Byte**		
12 bytes	0	-	C0/S0	not used	Control/status byte
	1	D1	D0	Mailbox (0, 6, 12 or 18 words)/ Process data (4 … 46 words)	
	…	…	…		
	5	D9	D8		
24 bytes	6	D11	D10		
	…	…	…		
	11	D21	D20		
48 bytes*)	12	D23	D22		
	...	...	...		
	23	D45	D44		

*) Factory Setting

16.2.5.17 Vibration Velocity/Bearing Condition Monitoring VIB I/O

750-645

The Vibration Velocity/Bearing Condition Monitoring VIB I/O has a total of 12 bytes of user data in both the Input and Output Process Image (8 bytes of module data and 4 bytes of control/status). The following table illustrates the Input and Output Process Image, which have 8 words mapped into each image. Word alignment is applied.

Table 265: Vibration Velocity/Bearing Condition Monitoring VIB I/O 750-645

Input and Output Process Image				
Offset	**Byte Destination**		**Description**	
	High Byte	**Low Byte**		
0	-	C0/S0	not used	Control/status byte (log. Channel 1, Sensor input 1)
1	D1	D0	Data bytes (log. Channel 1, Sensor input 1)	
2	-	C1/S1	not used	Control/status byte (log. Channel 2, Sensor input 2)
3	D3	D2	Data bytes (log. Channel 2, Sensor input 2)	
4	-	C2/S2	not used	Control/status byte (log. Channel 3, Sensor input 1)
5	D5	D4	Data bytes (log. Channel 3, Sensor input 3)	
6	-	C3/S3	not used	Control/status byte (log. Channel 4, Sensor input 2)
7	D7	D6	Data bytes (log. Channel 4, Sensor input 2)	

16.2.5.18 KNX/EIB/TP1 Module

753-646

The KNX/TP1 module appears in router and device mode with a total of 24-byte user data within the input and output area of the process image, 20 data bytes and 2 control/status bytes. Even though the additional bytes S1 or C1 are transferred as data bytes, they are used as extended status and control bytes. The opcode is used for the read/write command of data and the triggering of specific functions of the KNX/EIB/TP1 module. Word-alignment is used to assign 12 words in the process image. Access to the process image is not possible in router mode. Telegrams can only be tunneled.

In device mode, access to the KNX data can only be performed via special function blocks of the IEC application. Configuration using the ETS engineering tool software is required for KNX.

Table 266: KNX/EIB/TP1 Module 753-646

Input and Output Process Image				
Offset	**Byte Destination**		**Description**	
	High Byte	**Low Byte**		
0	-	C0/S0	not used	Control/Status byte
1	C1/S1	OP	extended Control/Status byte	Opcode
2	D1	D0	Data byte 1	Data byte 0
3	D3	D2	Data byte 3	Data byte 2
4	D5	D4	Data byte 5	Data byte 4
5	D7	D6	Data byte 7	Data byte 6
6	D9	D8	Data byte 9	Data byte 8
7	D11	D10	Data byte 11	Data byte 10
8	D13	D12	Data byte 13	Data byte 12
9	D15	D14	Data byte 15	Data byte 14
10	D17	D16	Data byte 17	Data byte 16
11	D19	D18	Data byte 19	Data byte 18

16.2.5.19 AS-interface Master Module

750-655,
753-655

The length of the process image of the AS-interface master module can be set to fixed sizes of 12, 20, 24, 32, 40 or 48 bytes.
It consists of a control or status byte, a mailbox with a size of 0, 6, 10, 12 or 18 bytes and the AS-interface process data, which can range from 0 to 46 bytes.

The AS-interface master module has a total of 6 to maximally 24 words data in both the Input and Output Process Image. Word alignment is applied.

The first Input and output word, which is assigned to an AS-interface master module, contains the status / control byte and one empty byte.

Subsequently the mailbox data are mapped, when the mailbox is permanently superimposed (Mode 1).

In the operating mode with suppressible mailbox (Mode 2), the mailbox and the cyclical process data are mapped next.
The following words contain the remaining process dat.

The mailbox and the process image sizes are set with the startup tool WAGO-I/O-*CHECK*.

Table 267: AS-interface Master Module 750-655, 753-655

Input and Output Process Image					
Process image size	**Offset**	**Byte Designation**		**Description**	
		High Byte	**Low Byte**		
12 bytes	0	-	C0/S0	Not used	Control-/ Status byte
	1	D1	D0	Mailbox (0, 6, 10, 12 or 18 bytes)/ Process data (0-46 bytes)	
	…				
	5	D9	D8		
20 bytes	6	D11	D10		
	…				
	9	D17	D16		
24 bytes *	10	D19	D18		
	11	D21	D20		
32 bytes	12	D23	D22		
	…				
	15	D29	D28		
40 bytes	16	D31	D30		
	…				
	19	D37	D36		
48 bytes	12	D39	D38		
	…				
	23	D45	D44		

*) Factory Setting

16.2.6 System Modules

16.2.6.1 System Modules with Diagnostics

750-606

The modules provide 2 bits of diagnostics in the Input Process Image for monitoring of the internal power supply.

Table 268: System Modules with Diagnostics 750-606, -611

Input Process Image							
Bit 7	**Bit 6**	**Bit 5**	**Bit 4**	**Bit 3**	**Bit 2**	**Bit 1**	**Bit 0**
						Diagnostics bit S_out	Diagnostics bit S_in

750-610, -611

The modules provide 2 bits of diagnostics in the Input Process Image for monitoring of the internal power supply.

Table 269: System Modules with Diagnostics 750-610, -611

Input Process Image							
Bit 7	**Bit 6**	**Bit 5**	**Bit 4**	**Bit 3**	**Bit 2**	**Bit 1**	**Bit 0**
						Diagnostics bit S 2 Fuse	Diagnostics bit S 1 Fuse

16.2.6.2 Filter Module

750-624/020-002, -626/020-002

The Filter Module 750-624/020-002 and 750-626/020-002 equipped with surge suppression for the field side power supply have a total of 8 bits in both the Input and Output Process Image.

Table 270: Filter Modules 750-624/020-002, 750-626/020-002

Input Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0V_MA	0V_PA	24V_MA	24V_PA	not used	PWR_DIAG	not used	VAL

Output Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
not used	not used	not used	not used	not used	not used	not used	GFT

16.2.6.3 Binary Space Module

750-622

The Binary Space Modules behave alternatively like 2 channel digital input modules or output modules and seize depending upon the selected settings 1, 2, 3 or 4 bits per channel. According to this, 2, 4, 6 or 8 bits are occupied then either in the process input or the process output image.

Table 271: Binary Space Module 750-622 (with Behavior like 2 Channel Digital Input)

Input and Output Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
(Data bit DI 8)	(Data bit DI 7)	(Data bit DI 6)	(Data bit DI 5)	(Data bit DI 4)	(Data bit DI 3)	Data bit DI 2	Data bit DI 1

List of Figures

Figure 1: View 27
Figure 2: Marking Area for Serial Numbers 29
Figure 3: Service Interface (Closed and Open Flap) 30
Figure 4: Network Connections – X1, X2 31
Figure 5: CAGE CLAMP® Connections (X3) 32
Figure 6: Data Contacts 33
Figure 7: Indicating elements for fieldbus/system 34
Figure 8: Indicating Elements, RJ-45 Jacks 35
Figure 9: Indicating Elements, Memory Card Slot 36
Figure 10: Address Selection Switch (here setting “0”) 37
Figure 11: Mode Selector Switch 38
Figure 12: Reset Button 39
Figure 13: MicroSD Card Slot 40
Figure 14: Schematic switching diagram 41
Figure 15: Example of Interface Assignment via WBM 48
Figure 16: Connecting the Controller to a Cloud Service (Example) 63
Figure 17: Spacing 75
Figure 18: Release Tab of Controller (Example) 77
Figure 19: Connecting a Conductor to a CAGE CLAMP® 78
Figure 20: Power Supply Concept 80
Figure 21: “Open DHCP”, Example Figure 85
Figure 22: CBM main menu (example) 86
Figure 23: CBM – Selecting “Networking” 87
Figure 24: CBM – Selecting “TCP/IP” 87
Figure 25: CBM – Selecting “IP address” 87
Figure 26: CBM – Selecting the IP Address 88
Figure 27: CBM – Entering a New IP Address 88
Figure 28: “WAGO Ethernet Settings” – Starting Screen (Example) 89
Figure 29: “WAGO Ethernet Settings” – “Network” Tab 90
Figure 30: Example of a Function Test 94
Figure 31: Entering Authentication 100
Figure 32: Password Reminder 102
Figure 33: WBM Browser Window (Example) 105
Figure 34: WBM Header with Tabs that Cannot be Displayed (Example) 105
Figure 35: WBM Status Bar (Example) 106
Figure 36: CBM main menu (example) 107
Figure 37: “WAGO Ethernet Settings” – Start Screen 111
Figure 38: “WAGO Ethernet Settings” – Communication Link 112
Figure 39: “WAGO Ethernet Settings” – Identification Tab (Example) 113
Figure 40: “WAGO Ethernet Settings” – Network Tab 114
Figure 41: “WAGO Ethernet Settings” – Protocol Tab 116
Figure 42: “WAGO Ethernet Settings” – Status Tab 117
Figure 43: Remanent Main Memory 120
Figure 44: Modbus Address Overview 121
Figure 45: State Diagram, ADVANCED_WATCHDOG Operation Mode 124
Figure 46: State Diagram, SIMPLE_WATCHDOG Operation Mode 125
Figure 47: State Diagram, Switching Operation Modes 125

Figure 48: Indicating elements for fieldbus/system 133
Figure 49: Indicating Elements, RJ-45 Jacks....138
Figure 50: Indicating Elements, Memory Card Slot....139
Figure 51: Flashing Sequence Process Diagram....140
Figure 52: Inserting the Memory Card 149
Figure 53: Release Tab of Controller....156
Figure 54: Marking Example According to ATEX and IECEx 160
Figure 55: Text Detail – Marking Example According to ATEX and IECEx 160
Figure 56: Marking Example for Approved I/O Module Ex i According to ATEX and IECEx....162
Figure 57: Text Detail – Marking Example for Approved I/O ModuleEx i According to ATEX and IECEx....162
Figure 58: Marking Example According to NEC....164
Figure 59: Text Detail – Marking Example According to NEC 500 164
Figure 60: Text Detail – Marking Example for Approved I/O Module Ex i According to NEC 505....165
Figure 61: Text Detail – Marking Example for Approved I/O Module Ex i According to NEC 506....165
Figure 62: Text Detail – Marking Example for Approved I/O Module Ex i According to CEC 18 attachment J 166

List of Tables

Table 1: Number Notation 16
Table 2: Font Conventions 16
Table 3: Legend for Figure “View” 27
Table 4: Service Interface 30
Table 5: Legend for Figure “Network Connections – X1, X2” 31
Table 6: Legend for Figure “CAGE CLAMP® Connections (X3)” 32
Table 7: Legend for Figure “Fieldbus/System Indicating Elements” 34
Table 8: Legend for Figure “Indicating Elements, RJ-45 Jacks” 35
Table 9: Legend for Figure “Indicating Elements, Memory Card Slot” 36
Table 10: Significance of the Address Values of the Address Selection Switch ..37
Table 11: Mode Selector Switch 38
Table 12: Technical Data – Mechanical Data 42
Table 13: Technical Data – System Data 42
Table 14: Technical Data – Power Supply 42
Table 15: Technical Data – Clock 43
Table 16: Technical Data – Programming 43
Table 17: Technical Data – Local Bus 43
Table 18: Technical Data – ETHERNET 43
Table 19: Technical Data – Field Wiring 44
Table 20: Technical Data – Data Contacts 44
Table 21: Technical Data – Climatic Environmental Conditions 44
Table 22: Services and Users 50
Table 23: WBM Users 51
Table 24: Linux Users 52
Table 25: List of Parameters Transmitted via DHCP 61
Table 26: Components of the Cloud Connectivity Software Package 64
Table 27: Loading a Boot Project 71
Table 28: WAGO DIN Rails 75
Table 29: Filter Modules for 24 V Supply 80
Table 30: Default IP Addresses for ETHERNET Interfaces 84
Table 31: Network Mask 255.255.255.0 84
Table 32: Significance of the Address Values of the Address Selection Switch ..91
Table 33:User Settings in the Default State 102
Table 34: Access Rights for WBM Pages 103
Table 35: CBM Menu Structure 108
Table 36: CODESYS V3 Priorities 119
Table 37: WAGO Modbus Registers 122
Table 38: Watchdog Commands 126
Table 39: Watchdog Status 127
Table 40: Watchdog Configuration 128
Table 41: Diagnostics via SYS LED 133
Table 42: RUN LED Diagnostics 134
Table 43: Diagnostics I/O LED 136
Table 44: MS-LED Diagnostics 137
Table 45: LNK-LED Diagnostics 138
Table 46: ACT-LED Diagnostics 138
Table 47: Diagnostics via Memory Card Slot LED 139

Table 48: Overview of Error Codes, I/O LED 142
Table 49: Error Code 1, Explanation of Blink Codes and Procedures for Troubleshooting 143
Table 50: Error Code 2, Explanation of Blink Codes and Procedures for Troubleshooting 144
Table 51: Error Code 3, Explanation of Blink Codes and Procedures for Troubleshooting 145
Table 52: Error Code 4, Explanation of Blink Codes and Procedures for Troubleshooting 146
Table 53: Error Code 5, Explanation of Blink Codes and Procedures for Troubleshooting 146
Table 54: Error Code 7, Explanation of Blink Codes and Procedures for Troubleshooting 146
Table 55: Error Code 9, Explanation of Blink Codes and Procedures for Troubleshooting 147
Table 56: Overview of MS-LED Error Codes 148
Table 57: Error Code 1, Explanation of Blink Codes and Procedures for Troubleshooting 148
Table 58: Description of Marking Example According to ATEX and IECEx 161
Table 59: Description of Marking Example for Approved I/O Module Ex I According to ATEX and IECEx 163
Table 60: Description of Marking Example According to NEC 500 164
Table 61: Description of Marking Example for Approved I/O Module Ex i According to NEC 505 165
Table 62: Description of Marking Example for Approved I/O Module Ex i According to NEC 506 165
Table 63: Description of Marking Example for Approved I/O Module Ex i According to CEC 18 attachment J 166
Table 64: WBM “Device Status” Page – “Device Details” Group 170
Table 65: WBM “Device Status” Page – “Network TCP/IP Details” Group 171
Table 66: WBM “PLC Runtime Information” Page – “Runtime” Group 173
Table 67: WBM “PLC Runtime Information” Page – “Project Details” Group 174
Table 68: WBM “PLC Runtime Information” Page – “Task n” Group(s) 174
Table 69: WBM “PLC Runtime Configuration” Page – “General PLC Runtime Configuration” Group 180
Table 70: WBM “PLC Runtime Configuration” Page – “Webserver Configuration” Group 182
Table 71: WBM “TCP/IP Configuration” Page – “TCP/IP Configuration” Group 183
Table 72: WBM “TCP/IP Configuration” Page – “DNS Server” Group 184
Table 73: WBM “Ethernet Configuration” Page – “Bridge Configuration” Group 185
Table 74: WBM “Ethernet Configuration” Page – “Switch Configuration” Group 186
Table 75: WBM “Ethernet Configuration” Page – “Ethernet Interface Configuration” Group 187
Table 76: WBM “Configuration of Host and Domain Name” Page – “Hostname” Group 188
Table 77: WBM “Configuration of Host and Domain Name” Page – “Domain Name” Group 188

Table 78: WBM “Routing” Page – “IP Forwarding through multiple interfaces” Group....190
Table 79: WBM “Routing” Page – “Custom Routes“ Group....191
Table 80: WBM “Routing” Page – “IP-Masquerading” Group....193
Table 81: WBM “Routing” Page – “Port Forwarding” Group....194
Table 82: WBM “Clock Settings” Page – “Timezone and Format” Group....195
Table 83: WBM “Clock Settings” Page – “UTC Time and Date” Group....195
Table 84: WBM “Clock Settings” Page – “Local Time and Date” Group....196
Table 85: WBM “Configuration of Service Interface” Page – “Assign Owner of Service Interface” Group....197
Table 86: WBM “Create Bootable Image” Page – “Create bootable image from active partition” Group....198
Table 87: WBM “Firmware Backup” Page – “Firmware Backup” Group....199
Table 88: WBM “Firmware Restore” Page – “Firmware Restore” Group....201
Table 89: WBM “Active System” Page – “Boot Device” Group....203
Table 90: WBM “Active System” Page – “System <n> (Internal Flash)” Group....203
Table 91: WBM “Mass Storage” Page – “Devices” Group....204
Table 92: WBM “Mass Storage” Page – “Create new Filesystem on Memory Card” Group....204
Table 93: WBM “Software Uploads” Page – “Upload New Software” Group....205
Table 94: WBM “Configuration of Network Services” Page – “FTP” Group....206
Table 95: WBM “Configuration of Network Services” Page – “FTPS (explicit FTPS)” Group....206
Table 96: WBM “Configuration of Network Services” Page – “HTTP” Group....207
Table 97: WBM “Configuration of Network Services” Page – “HTTPS” Group....207
Table 98: WBM “Configuration of Network Services” Page – “I/O-*CHECK*“ Group....207
Table 99: WBM “Configuration of NTP Client” Page – “NTP Client Configuration” Group....208
Table 100: WBM “PLC Runtime Services” Page – “CODESYS V2” Group....209
Table 101: WBM “PLC Runtime Services” Page – “***e!****RUNTIME*” Group....210
Table 102: WBM “SSH Server Settings” Page – “SSH Server” Group....211
Table 103: WBM “DHCP Server Configuration” Page – “DHCP Configuration Bridge <n>” Group....212
Table 104: WBM “Configuration of DNS Server” Page – “DNS Server” Group....213
Table 105: WBM “Status Overview” Page – “Service” Group....214
Table 106: WBM “Status Overview” Page – “Connection <n>” Group....214
Table 107: WBM “Configuration of Connection <n>” Page – “Configuration” Group....215
Table 108: Display of the Selection and Input Fields Depending on the Selected Cloud Platform....217
Table 109: Choice of Data Protocol Depending on the Selected Cloud Platform....219
Table 110: Display of the Selection and Input Fields Depending on the Selected Data Protocol....219
Table 111: Choice of Cache Mode Depending on the Selected Data Protocol....219
Table 112: Display of the Selection and Input Fields Depending on the Selected Authentication....220
Table 113: WBM “Configuration of General SNMP Parameters” Page – “General SNMP Configuration” Group....221

Table 114: WBM “Configuration of SNMP v1/v2c Parameters” Page – “SNMP v1/v2c Manager Configuration” Group....222
Table 115: WBM “Configuration of SNMP v1/v2c Parameters” Page – “Actually Configured Trap Receivers” Group....223
Table 116: WBM “Configuration of SNMP v3” Page – “Actually configured v3 Users” Group....224
Table 117: WBM “WBM User Configuration” Page – “Change Password” Group....226
Table 118: WBM “OPC UA Status” Page – “OPC UA Server” Group....227
Table 119: WBM “OPC UA Configuration” Page – “General OPC UA Server Configuration” Group....228
Table 120: WBM page “OPC UA Configuration” – group “OPC UA Endpoint URL”....228
Table 121: WBM “OPC UA Configuration” Page – “OPC UA Endpoints” Group....229
Table 122: WBM Page “OPC UA Configuration” – “OPC UA Security Settings” Group....230
Table 123: WBM Page “OPC UA Server Certificates” – “OPC UA Server Own Certificate” Group....231
Table 124: WBM Page “OPC UA Server Certificates” – “OPC UA Server Private Keys” Group....231
Table 125: WBM Page “OPC UA Server Certificates” – “OPC UA Server Trusted / Rejected Certificates” Group....232
Table 126: WBM “Modbus Services Configuration” Page – “Modbus TCP” Group....233
Table 127: WBM “Modbus Services Configuration” Page – “Modbus UDP” Group....233
Table 128: WBM “OpenVPN / IPsec Configuration” Page – “OpenVPN” Group....234
Table 129: WBM “OpenVPN / IPsec Configuration” Page – “IPsec” Group....235
Table 130: WBM “General Firewall Configuration” Page – “Global Firewall Parameter” Group....236
Table 131: WBM “Interface Configuration” Page – “Firewall Configuration Bridge <n> / VPN / WAN” Group....237
Table 132: WBM “Configuration of MAC Address Filter” Page – “Global MAC address filter state” Group....238
Table 133: WBM “Configuration of MAC Address Filter” Page – “MAC address filter state Bridge <n>” Group....239
Table 134: WBM “Configuration of MAC Address Filter” Page – “MAC address filter whitelist” Group....239
Table 135: WBM “Configuration of User Filter” Page – “User Filter” Group....240
Table 136: WBM “Configuration of OpenVPN and IPsec” Page – “Certificate List” Group....242
Table 137: WBM “Configuration of OpenVPN and IPsec” Page – “Private Key List” Group....242
Table 138: “Security Settings” WBM Page – “TLS Configuration” Group....243
Table 139: WBM “Advanced Intrusion Detection Environment (AIDE)” Page – “Run AIDE check at startup” Group....244
Table 140: WBM “Advanced Intrusion Detection Environment (AIDE)” Page – “Control AIDE and show log” Group....244

Table 141: WBM “Diagnostic Information” Page....246
Table 142: “Information” Menu....247
Table 143: “Information” > “Controller Details” Submenu....247
Table 144: “Information” > “Network Details” Submenu....248
Table 145: “PLC Runtime” Menu....249
Table 146: “PLC Runtime” > “Information” Submenu....249
Table 147: “PLC Runtime” > “Information” > “Runtime Version” Submenu....249
Table 148: “PLC Runtime” > “General Configuration” Submenu....250
Table 149: “PLC Runtime” > “General Configuration” > “PLC Runtime Version” Submenu....250
Table 150: “PLC Runtime” > “General Configuration” > “Home Dir On SD Card” Submenu....251
Table 151: “PLC Runtime” > “WebVisu” Submenu....252
Table 152: “Networking” Menu....253
Table 153: “Networking” > “Host/Domain Name” Submenu....253
Table 154: “Networking” > “Hostname” Submenu....254
Table 155: “Networking” > “Host/Domain Name” > “Domain Name” Submenu....254
Table 156: “Networking” > “TCP/IP” Submenu....254
Table 157: “Networking” > “IP Address” Submenu....255
Table 158: “Networking” > “TCP/IP” > “IP Address” Submenu > “Xn”....255
Table 159: “Networking” > “TCP/IP” > “Default Gateway” Submenu....256
Table 160: “Networking” > “TCP/IP” > “Default Gateway” > “Default Gateway n” Submenu....256
Table 161: “Networking” > “TCP/IP” > “DNS Server” Submenu....257
Table 162: “Networking” > “Ethernet” Submenu....257
Table 163: “Networking” > “Ethernet” > “Switch Configuration” Submenu....258
Table 164: “Networking” > “Ethernet” > “Ethernet Ports” Submenu....258
Table 165: “Networking” > “Ethernet” > “Ethernet Ports” > “Interface Xn” Submenu....259
Table 166: “Firewall” Menu....260
Table 167: “Firewall” > “General Configuration” Submenu....261
Table 168: “Firewall” > “General Configuration” > “Interface xxx” Submenu....262
Table 169: “Firewall” > “MAC Address Filter” Submenu....264
Table 170: “Firewall” > “MAC Address Filter” > “MAC address filter whitelist” Submenu....265
Table 171: “Firewall” > “MAC Address Filter” > “MAC address filter whitelist” > “Add new / No (n)” Submenu....265
Table 172: “Firewall” > “User Filter” Submenu....266
Table 173: “Firewall” > “User Filter” > “Add New / No (n)” Submenu....267
Table 174: “Clock” Menu....268
Table 175: “Administration” Menu....269
Table 176: “Administration” > “Users” Submenu....270
Table 177: “Administration” > “Create Image” Submenu....270
Table 178: “Package Server” Menu....271
Table 179: “Package Server” > “Firmware Backup” Menu....271
Table 180: “Package Server” > “Firmware Backup” > “Auto Update Feature” Menu....272
Table 181: “Package Server” > “Firmware Backup” > “Auto Update Feature” Menu....272
Table 182: “Package Server” > “Firmware Restore” Menu....273

Table 183: “Package Server” > “Firmware Restore” > “Select Package” Menu.273
Table 184: “Package Server” > “System Partition” Submenu 274
Table 185: “Mass Storage” Menu 275
Table 186: “Mass Storage” > “SD Card” Menu 275
Table 187: “Ports and Services” Menu 277
Table 188: “Ports and Services” > “Telnet” Submenu.....278
Table 189: “Ports and Services” > “FTP” Submenu 278
Table 190: “Ports and Services” > “FTPS” Submenu.....279
Table 191: “Ports and Services” > “HTTP” Submenu 279
Table 192: “Ports and Services” > “HTTPS” Submenu 280
Table 193: “Ports and Services” > “NTP” Submenu.....280
Table 194: “Ports and Services” > “SSH” Submenu 281
Table 195: “Ports and Services” > “TFTP” Submenu.....281
Table 196: “Ports and Services” > “DHCPD” Submenu 282
Table 197: “Ports and Services” > “DHCPD” > “Xn” Submenu 282
Table 198: “Ports and Services” > “DNS” Submenu 283
Table 199: “Ports and Services” > “IOCHECK PORT” Submenu.....284
Table 200: “Ports and Services” > “Modbus TCP” Submenu 284
Table 201: “Ports and Services” > “Modbus UDP” Submenu.....285
Table 202: “Ports and Services” > “OPC UA” Submenu 285
Table 203: “Ports and Services” > “Firewall Status” Submenu.....286
Table 204: “Ports and Services” > “PLC Runtime Services” Submenu 287
Table 205: “Ports and Services” > “PLC Runtime Services” > “e!RUNTIME” Submenu 287
Table 206: “SNMP” Menu.....288
Table 207: “SNMP” > “General SNMP Configuration” Submenu 288
Table 208: “SNMP” > “SNMP v1/v2c Manager Configuration” Submenu.....289
Table 209: “SNMP” > “SNMP v1/v2c Trap Receiver Configuration” Submenu..289
Table 210: “SNMP” > “SNMP v3 Configuration” Submenu 290
Table 211: “SNMP” > “(Secure)SNMP firewalling” Submenu.....291
Table 212: 1 Channel Digital Input Module with Diagnostics 293
Table 213: 2 Channel Digital Input Modules 293
Table 214: 2 Channel Digital Input Module with Diagnostics 293
Table 215: 2 Channel Digital Input Module with Diagnostics and Output Process Data 294
Table 216: 4 Channel Digital Input Modules 294
Table 217: 8 Channel Digital Input Modules 294
Table 218: 8 Channel Digital Input Module NAMUR with Diagnostics and Output Process Data 295
Table 219: 8 Channel Digital Input Module PTC with Diagnostics and Output Process Data 296
Table 220: 16 Channel Digital Input Modules 297
Table 221: 1 Channel Digital Output Module with Input Process Data.....298
Table 222: 2 Channel Digital Output Modules 298
Table 223: 2 Channel Digital Input Modules with Diagnostics and Input Process Data 299
Table 224: 2 Channel Digital Input Modules with Diagnostics and Input Process Data 75x-506 299
Table 225: 4 Channel Digital Output Modules 300

Table 226: 4 Channel Digital Output Modules with Diagnostics and Input Process Data 300
Table 227: 8 Channel Digital Output Module 300
Table 228: 8 Channel Digital Output Modules with Diagnostics and Input Process Data 301
Table 229: 16 Channel Digital Output Modules 301
Table 230: 8 Channel Digital Input/Output Modules 302
Table 231: 1 Channel Analog Input Modules 303
Table 232: 2 Channel Analog Input Modules 303
Table 233: 2-Channel Analog Input Modules HART 305
Table 234:: 2 Channel Analog Input Modules HART + 6 bytes Mailbox 305
Table 235: 4 Channel Analog Input Modules 305
Table 236: 8 Channel Analog Input Modules 306
Table 237: 3-Phase Power Measurement Module 307
Table 238: 3-Phase Power Measurement Modules 750-494, -495, (and all variations) 308
Table 239: 2 Channel Analog Output Modules 309
Table 240: 4 Channel Analog Output Modules 309
Table 241: Counter Modules 750-404, (and all variations except of /000-005), 753-404, -404/000-003 310
Table 242: Counter Modules 750-404/000-005, 753-404/000-005 311
Table 243: Counter Modules 750-633 312
Table 244: Counter Modules 750-638, 753-638 312
Table 245: Pulse Width Modules 750-511, /xxx-xxx, 753-511 313
Table 246: Serial Interface Modules with Alternative Data Format 314
Table 247: Serial Interface Modules with Standard Data Format 314
Table 248: Serial Interface Modules 750-652, 753-652 315
Table 249: Data Exchange Module 750-654, -654/000-001 315
Table 250: SSI Transmitter Interface Modules 316
Table 251: SSI Transmitter Interface I/O Modules with an Alternative Data Format (/000-004, -005, -007) 316
Table 252: Incremental Encoder Interface Modules 750-631/000-004, --010, -011 316
Table 253: Incremental Encoder Interface Modules 750-634 317
Table 254: Incremental Encoder Interface Modules 750-637, (and all variations) 317
Table 255: Digital Pulse Interface Modules 750-635, 753-635 318
Table 256: DC-Drive Controller 750-636, -636/000-700, -636/000-800 318
Table 257: Stepper Controller 750-670, -671, -672 319
Table 258: RTC Module 750-640 320
Table 259: DALI Multi-Master Module 753-647 in the "Easy" Mode 321
Table 260: DALI Multi-Master Module 753-647 in the "Full" Mode 323
Table 261: LON® FTT Module 753-648 324
Table 262: EnOcean Radio Receiver 750-642 324
Table 263: MP Bus Master Module 750-643 325
Table 264: *Bluetooth*® RF-Transceiver 750-644 326
Table 265: Vibration Velocity/Bearing Condition Monitoring VIB I/O 750-645 326
Table 266: KNX/EIB/TP1 Module 753-646 327
Table 267: AS-interface Master Module 750-655, 753-655 328
Table 268: System Modules with Diagnostics 750-606, -611 329

Table 269: System Modules with Diagnostics 750-610, -611.....329
Table 270: Filter Modules 750-624/020-002, 750-626/020-002 329
Table 271: Binary Space Module 750-622 (with Behavior like 2 Channel Digital Input).....330

WAGO GmbH & Co. KG
Postfach 2880 • D - 32385 Minden
Hansastraße 27 • D - 32423 Minden
Phone: +49 571 887 – 0
Fax: +49 571 887 – 844169
E-Mail: info@wago.com
Internet: www.wago.com