

WAGO-I/O-SYSTEM 750



750-8212/0000-0100

PFC200; G2; 2ETH RS BACnet/IP

**Controller PFC200; Generation 2; 2 x ETHERNET,
RS-232/-485; BACnet/IP**

© 2019 WAGO Kontakttechnik GmbH & Co. KG
All rights reserved.

The contents of this documentation are taken in part from the BACnet Standard 135-2012 or are based on the original contents. These contents are subject to copyright.

The following applies to these contents: ©2012, American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc. (www.ashrae.org).
Reprinted by permission from 2012 ASHRAE Standard-135. This material may not be copied nor distributed in either paper or digital form without ASHRAE's permission.

WAGO Kontakttechnik 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 – 445 55
Fax: +49 (0) 571/8 87 – 8 445 55

E-Mail: support.de@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	13
1.1	Validity of this Documentation.....	13
1.2	Copyright.....	13
1.3	Property rights.....	14
1.4	Symbols	15
1.5	Number Notation.....	17
1.6	Font Conventions.....	17
2	Important Notes	18
2.1	Legal Bases	18
2.1.1	Subject to Changes	18
2.1.2	Personnel Qualifications.....	18
2.1.3	Use of the 750 Series in Compliance with Underlying Provisions.....	18
2.1.4	Technical Condition of Specified Devices	19
2.2	Safety Advice (Precautions).....	20
2.3	Licensing Terms of the Software Package Used	23
2.4	Special Use Conditions for ETHERNET Devices	23
3	Device Description	25
3.1	View	29
3.2	Labeling	31
3.2.1	Labeling Symbols.....	31
3.2.2	Manufacturing Number.....	32
3.2.3	Hardware Address (MAC-ID)	33
3.2.4	Update Matrix.....	33
3.3	Connectors.....	34
3.3.1	Data Contacts/Local Bus.....	34
3.3.2	Power Jumper Contacts/Field Supply	35
3.3.3	CAGE CLAMP® Connectors.....	36
3.3.4	Service Interface	37
3.3.5	Network Connectors.....	38
3.3.6	Communication Interface	39
3.3.6.1	Operating as an RS-232 Interface	40
3.3.6.2	Operating as an RS-485 Interface	41
3.4	Display Elements	42
3.4.1	Power Supply Indicating Elements.....	42
3.4.2	Fieldbus/System Indicating Elements	43
3.4.3	Memory Card Indicating Elements	44
3.4.4	Network Indicating Elements.....	45
3.5	Operating Elements	46
3.5.1	Operating Mode Switch	46
3.5.2	Reset Button	47
3.6	Slot for Memory Card.....	48
3.7	Schematic Diagram.....	49
3.8	Technical Data	50
3.8.1	Mechanical Data.....	50
3.8.2	System Data.....	50
3.8.3	Power Supply	50

3.8.4	Clock	51
3.8.5	Programming.....	51
3.8.6	Local Bus	51
3.8.7	ETHERNET	52
3.8.8	BACnet/IP	52
3.8.9	Communication Interface	53
3.8.10	Connection Type	53
3.8.11	Climatic Environmental Conditions.....	54
3.8.12	Software Compatibility.....	54
3.9	Approvals	55
3.10	Standards and Guidelines.....	57
3.11	BACnet-Building-Controller (B-BC).....	58
3.11.1	BIBBs (BACnet Interoperability Building Blocks).....	59
3.11.2	Data Sharing BIBBs	61
3.11.3	Alarm and Event Management BIBBs.....	63
3.11.4	Scheduling BIBBs.....	65
3.11.5	Trending BIBBs	65
3.11.6	Device- und Network-Management-BIBBs.....	67
4	Function Description.....	71
4.1	Network.....	71
4.1.1	Interface Configuration	71
4.1.1.1	Operation in Switch Mode	71
4.1.1.2	Operation with Separate Network Interfaces	71
4.1.2	Network Security	72
4.1.2.1	Users and Passwords.....	72
4.1.2.1.1	Services and Users	72
4.1.2.1.2	WBM User Group.....	73
4.1.2.1.3	Linux® User Group	73
4.1.2.1.4	SNMP User Group	73
4.1.2.2	Web Protocols for WBM Access.....	74
4.1.2.2.1	TLS Encryption	74
4.1.2.3	Root Certificates	76
4.1.3	Network Configuration.....	77
4.1.3.1	Host Name/Domain Name	77
4.1.4	Routing.....	77
4.1.5	Network Services	80
4.1.5.1	DHCP Client	80
4.1.5.2	DHCP Server.....	80
4.1.5.3	DNS Server	82
4.1.6	Cloud Connectivity Functionality	83
4.1.6.1	Components of the Cloud Connectivity Software Package	84
4.2	Memory Card Function	85
4.2.1	Formatting	85
4.2.2	Data Backup.....	87
4.2.2.1	BACnet Data Assurance.....	87
4.2.2.2	Backup Function	88
4.2.2.3	Restore Function	89
4.2.3	Inserting a Memory Card during Operation	91
4.2.4	Removing the Memory Card during Operation.....	91

4.2.5	Setting the Home Directory for the Runtime System.....	92
4.2.6	Load Boot Project.....	93
5	Mounting	94
5.1	Installation Position	94
5.2	Overall Configuration	94
5.3	Mounting onto Carrier Rail	96
5.3.1	Carrier Rail Properties.....	96
5.3.2	WAGO DIN Rails.....	97
5.4	Spacing	97
5.5	Mounting Sequence	98
5.6	Inserting Devices	99
5.6.1	Inserting the Controller	99
6	Connect Devices.....	100
6.1	Connecting a Conductor to the CAGE CLAMP®	100
6.2	Power Supply Concept	101
6.2.1	Overcurrent Protection	101
6.2.2	Supplementary Power Supply Regulations	102
7	Commissioning.....	103
7.1	Switching On the Controller	103
7.2	Determining the IP Address of the Host PC.....	104
7.3	Setting an IP Address	105
7.3.1	Assigning an IP Address using DHCP	106
7.3.2	Changing an IP Address using “WAGO Ethernet Settings”	107
7.3.3	Temporarily Setting a Fixed IP Address.....	109
7.4	Testing the Network Connection.....	110
7.5	Changing Passwords	111
7.6	Shutdown/Restart	112
7.7	Initiating Reset Functions.....	113
7.7.1	Warm Start Reset.....	113
7.7.2	Cold Start Reset.....	113
7.7.3	Software Reset.....	113
7.8	Configuration.....	114
7.8.1	Configuration via Web-Based-Management (WBM)	115
7.8.1.1	WBM User Administration	116
7.8.1.2	General Information about the Page	119
7.8.1.3	“Status Information” Page.....	121
7.8.1.3.1	“Controller Details” Group	121
7.8.1.3.2	“Network Details Xn” Group(s).....	121
7.8.1.4	“PLC Runtime Information” Page	123
7.8.1.4.1	“PLC Runtime” Group	123
7.8.1.5	“General PLC Runtime Configuration” Page	124
7.8.1.5.1	“General PLC Runtime Configuration” Group	124
7.8.1.6	“PLC WebVisu” Page	125
7.8.1.6.1	“Webserver Configuration” Group.....	125
7.8.1.7	“Configuration of Host and Domain Name” Page	126
7.8.1.7.1	“HostName” Group.....	126
7.8.1.7.2	“Domain Name” Group.....	127
7.8.1.8	“TCP/IP Configuration” Page.....	128

7.8.1.8.1	"IP Configuration (Xn)" Group(s).....	128
7.8.1.8.2	"Default Gateway n" Groups	129
7.8.1.8.3	"DNS Server" Group	130
7.8.1.9	"Ethernet Configuration" Page	131
7.8.1.9.1	"Switch Configuration" Group.....	131
7.8.1.9.2	"Interface Xn" Groups	132
7.8.1.10	"Routing" Page	133
7.8.1.10.1	"General Routing Configuration" Group	133
7.8.1.10.2	"Static Routes" Group	134
7.8.1.10.3	"Dynamic Routes" Group	135
7.8.1.10.4	"IP Masquerading" Group	135
7.8.1.10.5	"Port Forwarding" Group	136
7.8.1.11	"General Firewall Configuration" Page	137
7.8.1.11.1	"Global Firewall Parameters" Group	137
7.8.1.11.2	"Firewall Parameters Interface xxx" Group	138
7.8.1.12	"Configuration of MAC Address Filter" Page	139
7.8.1.12.1	"Global MAC Address Filter State" Group.....	139
7.8.1.12.2	"MAC Address Filter State Xn" Group.....	140
7.8.1.12.3	"MAC Address Filter Whitelist" Group	140
7.8.1.13	"Configuration of User Filter" Page	141
7.8.1.13.1	"User Filter" Group	141
7.8.1.13.2	"User Filter n" Group	141
7.8.1.13.3	"Add New User Filter" Group	142
7.8.1.14	"Configuration of Time and Date" Page	143
7.8.1.14.1	"Date on Device" Group	143
7.8.1.14.2	"Time on Device" Group.....	143
7.8.1.14.3	"Time Zone" Group	144
7.8.1.14.4	"TZ String" Group.....	145
7.8.1.15	"Configuration of the Users for the Web-based Management" Page.....	146
7.8.1.15.1	"Change Password for Selected User" Group	146
7.8.1.16	"Create Bootable Image" Page.....	147
7.8.1.16.1	"Create Bootable Image from Active Partition (<Active Partition>)" Group	147
7.8.1.17	"Configuration of Serial Interface RS232" Page	149
7.8.1.17.1	"Serial Interface Assigned to" Group.....	149
7.8.1.17.2	"Assign Owner of Serial Interface (Active after Next Controller Reboot)" Group	149
7.8.1.18	"Configuration of Service Interface" Page	150
7.8.1.18.1	"Service Interface assigned to" Group	150
7.8.1.18.2	"Assign Owner of Service Interface (enabled after next controller reboot)" Group.....	150
7.8.1.19	"Reboot Controller" Page.....	151
7.8.1.19.1	"Reboot Controller" Group	151
7.8.1.20	"Firmware Backup" Page.....	152
7.8.1.21	"Firmware Restore" Page	154
7.8.1.22	"System Partition" Page.....	156
7.8.1.22.1	"Current Active Partition" Group.....	156
7.8.1.22.2	"Set Inactive Partition Active" Group	156
7.8.1.23	"Mass Storage" Page.....	157
7.8.1.23.1	"<Device Name>" Group(s).....	157

7.8.1.23.2	"<Device Name> - create new filesystem" Group(s).....	157
7.8.1.24	"Software Uploads" Page	158
7.8.1.24.1	"Upload New Software" Group	158
7.8.1.24.2	"Activate New Software" Group	158
7.8.1.25	"Configuration of Network Services" Page	159
7.8.1.25.1	"Telnet" Group.....	159
7.8.1.25.2	"FTP" Group.....	159
7.8.1.25.3	"FTPS" Group	159
7.8.1.25.4	"HTTP" Group	160
7.8.1.25.5	"HTTPS" Group.....	160
7.8.1.25.6	"WAGO-I/O-CHECK" Group	160
7.8.1.25.7	"OPC UA" Group.....	161
7.8.1.26	"Configuration of NTP Client" Page	162
7.8.1.26.1	"NTP Client Configuration" Group	162
7.8.1.26.2	"NTP Single Request" Group	162
7.8.1.27	"Configuration of PLC Runtime Services" Page	163
7.8.1.27.1	"General Configuration" Group	163
7.8.1.27.2	"e!RUNTIME" Group	163
7.8.1.28	"SSH Server Settings" Page.....	164
7.8.1.28.1	"SSH Server" Group.....	164
7.8.1.29	"TFTP Server" Page	165
7.8.1.29.1	"TFTP Server" Group	165
7.8.1.30	"DHCP Configuration" Page	166
7.8.1.30.1	"DHCP Configuration Xn" Group.....	166
7.8.1.31	"Configuration of DNS Service" Page.....	167
7.8.1.31.1	"DNS Service" Group	167
7.8.1.32	"Modbus Services Configuration" Page	168
7.8.1.32.1	"Modbus TCP" Group.....	168
7.8.1.32.2	"Modbus UDP" Group	168
7.8.1.33	"Configuration of Cloud Connectivity" Page	169
7.8.1.33.1	"Software Version" Group	169
7.8.1.33.2	"Status" Group	169
7.8.1.33.3	"Settings" Group.....	170
7.8.1.34	"Configuration of General SNMP Parameters" Page.....	175
7.8.1.34.1	"General SNMP Configuration" Group	175
7.8.1.35	"Configuration of SNMP v1/v2c Parameters" Page	176
7.8.1.35.1	"SNMP v1/v2c Manager Configuration" Group	176
7.8.1.35.2	"Actually Configured Trap Receivers" Group(s).....	176
7.8.1.35.3	"Trap Receiver n" Group(s).....	177
7.8.1.35.4	"Add New Trap Receiver" Group	177
7.8.1.36	"Configuration of SNMP v3 Users" Page.....	178
7.8.1.36.1	"Actually Configured v3 Users" Group(s)	178
7.8.1.36.2	"v3 User n" Group(s)	178
7.8.1.36.3	"Add New v3 User" Group.....	179
7.8.1.37	"Diagnostic Information" Page	180
7.8.1.38	"Configuration of General BACnet" Page	181
7.8.1.38.1	"BACnet Status" Group.....	181
7.8.1.38.2	"BACnet General Parameter" Group.....	181
7.8.1.38.3	"BACnet Upload" Group.....	181
7.8.1.39	"Configuration of BACnet Storage Location parameters" Page..	182

7.8.1.39.1	“BACnet Persistence“ Group	182
7.8.1.39.2	“BACnet Trendlog“ Group	183
7.8.1.39.3	“BACnet Eventlog“ Group	183
7.8.1.40	“BACnet Diagnostic Information“ Page.....	184
7.8.1.41	“Configuration of OpenVPN and IPsec“ Page	185
7.8.1.41.1	“OpenVPN“ Group	185
7.8.1.41.2	“IPsec“ Group.....	185
7.8.1.41.3	“Certificate Upload“ Group	186
7.8.1.41.4	“Certificate List“ Group.....	186
7.8.1.41.5	“Private Key List“ Group.....	186
7.8.1.42	“Security Settings“ Page.....	187
7.8.1.42.1	“Transport Layer Security Settings“ Group	187
7.8.1.43	“Advanced Intrusion Detection Environment (AIDE) Page“	188
7.8.1.43.1	“Run AIDE check at startup“ Group	188
7.8.1.43.2	“Control AIDE and show log“ Group	188
7.8.1.44	“Open Source Licenses“ Page	189
7.8.1.45	“WAGO Licenses“ Page	190
7.8.2	Configuration via Console-Based-Management-Tool (CBM) using a Terminal Program.....	191
7.8.2.1	CBM Menu Structure Overview	193
7.8.2.2	“Information“ Menu	195
7.8.2.2.1	“Information“ > “Controller Details“ Submenu	195
7.8.2.2.2	“Information“ > “Network Details“ Submenu.....	196
7.8.2.3	“PLC Runtime“ Menu	197
7.8.2.3.1	“PLC Runtime“ > “Information“ Submenu	197
7.8.2.3.2	“Information“ > “Runtime Version“ Submenu	197
7.8.2.3.3	“PLC Runtime“ > “General Configuration“ Submenu	198
7.8.2.3.4	“General Configuration“ > “PLC Runtime Version“ Submenu	198
7.8.2.3.5	“General Configuration“ > “Home Dir On SD Card“ Submenu.....	199
7.8.2.3.6	“PLC Runtime“ > “WebVisu“ Submenu	200
7.8.2.4	“Networking“ Menu	201
7.8.2.4.1	“Networking“ > “Host/Domain Name“ Submenu	201
7.8.2.4.2	“Host/Domain Name“ > “Hostname“ Submenu	202
7.8.2.4.3	“Host/Domain Name“ > “Domain Name“ Submenu	202
7.8.2.4.4	“Networking“ > “TCP/IP“ Submenu	202
7.8.2.4.5	“TCP/IP“ > “IP Address“ Submenu.....	203
7.8.2.4.6	“IP Address“ > “Xn“ Submenu.....	203
7.8.2.4.7	“TCP/IP“ > “Default Gateway“ Submenu.....	204
7.8.2.4.8	“Default Gateway“ > “Default Gateway n“ Submenu.....	204
7.8.2.4.9	“TCP/IP“ > “DNS Server“ Submenu	205
7.8.2.4.10	“Networking“ > “Ethernet“ Submenu	205
7.8.2.4.11	“Ethernet“ > “Switch Configuration“ Submenu	206
7.8.2.4.12	“Ethernet“ > “Ethernet Ports“ Submenu	206
7.8.2.4.13	“Ethernet Ports“ > “Interface Xn“ Submenu	207
7.8.2.5	“Firewall“ Menu.....	208
7.8.2.5.1	“Firewall“ > “General Configuration“ Submenu	209
7.8.2.5.2	“General Configuration“ > “Interface xxx“ Submenu	210
7.8.2.5.3	“Firewall“ > “MAC Address Filter“ Submenu	212
7.8.2.5.4	“MAC Address Filter“ > “MAC address filter whitelist“ Submenu.....	213
7.8.2.5.5	“MAC address filter whitelist“ > “Add new / No (n)“ Submenu.....	213

7.8.2.5.6	“Firewall” > “User Filter” Submenu.....	214
7.8.2.5.7	“User Filter” > “Add New / No (n)” Submenu.....	215
7.8.2.6	“Clock” Menu	216
7.8.2.7	“Administration” Menu	217
7.8.2.7.1	“Administration” > “Users” Submenu.....	218
7.8.2.7.2	“Administration” > “Create Image” Submenu	218
7.8.2.8	“Package Server” Menu.....	219
7.8.2.8.1	“Package Server” > “Firmware Backup” Submenu	219
7.8.2.8.2	“Firmware Backup” > “Auto Update Feature” Submenu	220
7.8.2.8.3	“Firmware Backup” > “Destination” Submenu.....	220
7.8.2.8.4	“Package Server” > “Firmware Restore” Submenu.....	221
7.8.2.8.5	“Firmware Restore” > “Select Package” Submenu	221
7.8.2.8.6	“Package Server” > “System Partition” Submenu	222
7.8.2.9	“Mass Storage” Menu	223
7.8.2.9.1	“Mass Storage” > “SD Card” Submenu.....	223
7.8.2.10	“Software Uploads” Menu.....	224
7.8.2.11	“Ports and Services” Menu	225
7.8.2.11.1	“Ports and Services” > “Telnet” Submenu.....	226
7.8.2.11.2	“Ports and Services” > “FTP” Submenu	226
7.8.2.11.3	“Ports and Services” > “FTPS” Submenu	227
7.8.2.11.4	“Ports and Services” > “HTTP” Submenu	227
7.8.2.11.5	“Ports and Services” > “HTTPS” Submenu.....	228
7.8.2.11.6	“Ports and Services” > “NTP” Submenu	228
7.8.2.11.7	“Ports and Services” > “SSH” Submenu	229
7.8.2.11.8	“Ports and Services” > “TFTP” Submenu.....	229
7.8.2.11.9	“Ports and Services” > “DHCPD” Submenu.....	230
7.8.2.11.10	“DHCPD” > “Xn” Submenu.....	230
7.8.2.11.11	“Ports and Services” > “DNS” Submenu	231
7.8.2.11.12	“Ports and Services” > “IOCHECK PORT” Submenu	232
7.8.2.11.13	“Ports and Services” > “Modbus TCP” Submenu.....	232
7.8.2.11.14	“Ports and Services” > “Modbus UDP” Submenu	233
7.8.2.11.15	“Ports and Services” > “OPC UA” Submenu.....	233
7.8.2.11.16	“...” > “Firewall Status” Submenu.....	234
7.8.2.11.17	“Ports and Services” > “PLC Runtime Services” Submenu ...	235
7.8.2.11.18	“PLC Runtime Services” > “e!RUNTIME” Submenu	235
7.8.2.12	“SNMP” Menu.....	236
7.8.2.12.1	“SNMP” > “General SNMP Configuration” Submenu.....	236
7.8.2.12.2	“SNMP” > “SNMP v1/v2c Manager Configuration” Submenu	237
7.8.2.12.3	“SNMP” > “SNMP v1/v2c Trap Receiver Configuration” Submenu.....	237
7.8.2.12.4	“SNMP” > “SNMP v3 Configuration” Submenu.....	238
7.8.2.12.5	“SNMP” > “(Secure)SNMP firewalling” Submenu	239
7.8.3	Configuration using “WAGO Ethernet Settings”	240
7.8.3.1	Identification Tab	242
7.8.3.2	Network Tab	243
7.8.3.3	PLC Tab	245
7.8.3.4	Status Tab	246
8	e!RUNTIME Runtime Environment.....	247
8.1	General Notes.....	247

8.2	CODESYS V3 Priorities	248
8.3	Memory Spaces under <i>e!RUNTIME</i>	249
8.3.1	Program and Data Memory	249
8.3.2	Function Block Limitation	249
8.3.3	Remanent Memory	249
9	Modbus – e!RUNTIME	250
9.1	Modbus Address Overview	250
9.2	Modbus Registers	251
9.2.1	Modbus Watchdog	253
9.2.1.1	Register 0xFA00 – Watchdog Command	255
9.2.1.2	Register 0xFA01 – Watchdog Timeout	256
9.2.1.3	Register 0xFA02 – Watchdog Status	256
9.2.1.4	Register 0xFA03 – Watchdog Config	257
9.2.1.5	Modbus TCP Connection Watchdog Register	258
9.2.2	Status Registers	259
9.2.2.1	PLC Status Register	259
9.2.3	Electronic Nameplate	259
9.2.3.1	Order Number	259
9.2.3.2	Firmware Version	259
9.2.3.3	Hardware Version	259
9.2.3.4	Firmware Loader/Boot Loader	259
9.2.4	Modbus Process Image Version	259
9.2.5	Modbus Process Image Registers	259
9.2.6	Constant Registers	260
9.2.7	Live Register	260
9.3	Estimating the Modbus Master CPU Load	261
10	Diagnostics	262
10.1	Operating and Status Messages	262
10.1.1	Power Supply Indicating Elements	262
10.1.2	Fieldbus/System Indicating Elements	263
10.1.3	Network Indicating Elements	268
10.2	Diagnostics Messages via Flashing Sequences	269
10.2.1	Flashing Sequences	269
10.2.2	Example of a Diagnostics Message Indicated by a Flashing Sequence	271
10.2.3	Meaning of Blink Codes and Procedures for Troubleshooting	272
10.2.4	Meaning of Blink Codes and Procedures for Troubleshooting	278
11	Service	279
11.1	Inserting and Removing the Memory Card	279
11.1.1	Inserting the Memory Card	279
11.1.2	Removing the Memory Card	280
11.2	Firmware Changes	281
11.2.1	Perform Firmware Upgrade	281
11.2.2	Perform Firmware Downgrade	282
11.2.3	Factory Reset	283
11.3	Updating Root Certificates	284
12	Removal	285

12.1	Removing Devices	285
12.1.1	Removing the Controller.....	285
13	Disposal.....	286
13.1	Electrical and electronic equipment	286
13.2	Packaging	287
14	Use in Hazardous Environments	288
14.1	Marking Configuration Examples	289
14.1.1	Marking for Europe According to ATEX and IECEx	289
14.1.2	Marking for the United States of America (NEC) and Canada (CEC).....	293
14.2	Installation Regulations.....	296
14.2.1	Special Notes including Explosion Protection	296
14.2.2	Special Notes Regarding ANSI/ISA Ex	298
15	Appendix	299
15.1	Process Data Architecture	299
15.1.1	Digital Input Modules.....	300
15.1.1.1	1 Channel Digital Input Module with Diagnostics	300
15.1.1.2	2 Channel Digital Input Modules.....	300
15.1.1.3	2 Channel Digital Input Module with Diagnostics	300
15.1.1.4	2 Channel Digital Input Module with Diagnostics and Output Process Data	301
15.1.1.5	4 Channel Digital Input Modules.....	301
15.1.1.6	8 Channel Digital Input Modules.....	301
15.1.1.7	8 Channel Digital Input Module NAMUR with Diagnostics and Output Process Data	302
15.1.1.8	8 Channel Digital Input Module PTC with Diagnostics and Output Process Data	303
15.1.1.9	16 Channel Digital Input Modules.....	304
15.1.2	Digital Output Modules	305
15.1.2.1	1 Channel Digital Output Module with Input Process Data.....	305
15.1.2.2	2 Channel Digital Output Modules.....	305
15.1.2.3	2 Channel Digital Input Modules with Diagnostics and Input Process Data	306
15.1.2.4	4 Channel Digital Output Modules.....	307
15.1.2.5	4 Channel Digital Output Modules with Diagnostics and Input Process Data	307
15.1.2.6	8 Channel Digital Output Module.....	307
15.1.2.7	8 Channel Digital Output Modules with Diagnostics and Input Process Data	308
15.1.2.8	16 Channel Digital Output Modules	308
15.1.2.9	8 Channel Digital Input/Output Modules	309
15.1.3	Analog Input Modules	310
15.1.3.1	1 Channel Analog Input Modules	310
15.1.3.2	2 Channel Analog Input Modules	310
15.1.3.3	2 Channel Analog Input Modules HART	311
15.1.3.4	4 Channel Analog Input Modules	312
15.1.3.5	8 Channel Analog Input Modules	313
15.1.3.6	3-Phase Power Measurement Module	314
15.1.4	Analog Output Modules.....	316

15.1.4.1	2 Channel Analog Output Modules.....	316
15.1.4.2	4 Channel Analog Output Modules.....	316
15.1.5	Specialty Modules	317
15.1.5.1	Counter Modules	317
15.1.5.2	Pulse Width Modules	320
15.1.5.3	Serial Interface Modules with Alternative Data Format.....	320
15.1.5.4	Serial Interface Modules with Standard Data Format.....	321
15.1.5.5	Serial Interface Modules	321
15.1.5.6	Data Exchange Module	322
15.1.5.7	SSI Transmitter Interface Modules	322
15.1.5.8	Incremental Encoder Interface Modules	323
15.1.5.9	DC-Drive Controller	325
15.1.5.10	Stepper Controller	326
15.1.5.11	RTC Module	327
15.1.5.12	DALI Multi-Master Module	327
15.1.5.13	LON® FTT Module	331
15.1.5.14	EnOcean Radio Receiver	331
15.1.5.15	MP Bus Master Module	332
15.1.5.16	<i>Bluetooth</i> ® RF-Transceiver	332
15.1.5.17	Vibration Velocity/Bearing Condition Monitoring VIB I/O	333
15.1.5.18	KNX/EIB/TP1 Module	334
15.1.5.19	AS-interface Master Module	335
15.1.6	System Modules.....	336
15.1.6.1	System Modules with Diagnostics	336
15.1.6.2	Filter Module	336
15.1.6.3	Binary Space Module	337
Glossary		338
Literature List.....		357
List of Figures		358
List of Tables.....		360

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 “PFC200; G2; 2ETH RS BACnet/IP” controller (750-8212/0000-0100).

This documentation is only applicable from FW Version 03.02.02(14).

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 Kontakttechnik 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.
- AS-Interface® is a registered trademark of AS-International Association.
- BACnet® is a registered trademark of American Society of Heating, Refrigerating and Air Conditioning Engineers, Inc. (ASHRAE).
- *Bluetooth*® is a registered trademark of the Bluetooth SIG, Inc.
- CiA® and CANopen® are registered trademarks of CAN in AUTOMATION – International Users and Manufacturers Group e. V.
- DALI is a registered trademark of Digital Illumination Interface Alliance (DiiA).
- EtherCAT® is a registered trademark and patented technology of Beckhoff Automation GmbH.
- EtherNet/IP™ is a registered trademark of Open DeviceNet Vendor Association, Inc (ODVA).
- EnOcean® is a registered trademark of EnOcean GmbH.
- IO-Link is a registered trademark of PROFIBUS Nutzerorganisation e.V.
- KNX® is a registered trademark of KNX Association cvba.
- Linux® is a registered trademark of Linus Torvalds.
- LON® is a registered trademark of Echelon Corporation.
- Modbus® is a registered trademark of Schneider Electric, licensed to the Modbus Organization, Inc.
- PROFIBUS® is a registered trademark of Siemens AG.
- PROFINET® is a registered trademark of Siemens AG.
- Subversion® is a registered trademark of 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
<i>italic</i>	Names of paths and data files are marked in italic-type. e.g.: <i>C:\Program Files\WAGO Software</i>
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 Kontakttechnik GmbH & Co. KG reserves the right to provide for any alterations or modifications. WAGO Kontakttechnik 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 of 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.

This product is designed for protection class IP20. There is protection against finger injury and solid impurities up to 12.5 mm diameter is assured; protection against water damage is not ensured.

The product represents an open-type device. It 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)".

The product is intended for installation in automation systems. It does not have its own integrated separator. A suitable separator must therefore be created on the plant side.

The operation of the product in residential areas without further measures is only permitted if the product complies with the emission limits (interference emissions) according to EN 61000-6-3.

Operating the product in home applications without further measures is only permitted if it meets 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 fieldbus coupler/controller.

Appropriate housing (per 2014/34/EU) is required when operating the WAGO-I/O-SYSTEM 750 in hazardous environments. 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 Kontakttechnik 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 Kontakttechnik 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 only one 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.

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 “PFC200; G2; 2ETH RS BACnet/IP” controller (750-8212/0000-0100) 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 Kontakttechnik 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 Device Description

The controller 750-8212/0000-0100(PFC200; G2; 2ETH RS BACnet/IP) 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.

The controller connects the WAGO I/O-SYSTEM with the BACnet protocol. The controller complies with the BACnet device profile "BACnet Building Controller" B-BC in accordance with DIN EN ISO 16484-5 and has 2 functions available internally:

- 1 BACnet objects that are created by the controller as standard (Device, file objects, etc.).
- 2 BACnet objects that are created via the WAGO BACnet Configurator (WBC) or the PLC program.

This BACnet/IP controller can be used for applications in building technology.

The controller is configured and commissioned using the WAGO BACnet Configurator.

For the IEC 61131-3 programming of the applications, the CODESYS 3-based programming system *e!COCKPIT*, which uses the runtime environment *e!RUNTIME*, is available as engineering software.



Information

Additional Information about the Configuration and Programming Software

The BACnet Configurator and the engineering software *e!COCKPIT* and the documentation for this can be downloaded from the website for this product under <http://www.wago.com>.

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 60 MB of program and data memory (dynamically distributed) and 128 kB of retentive memory (retain and flag variables) in an integrated NVRAM.

Two ETHERNET interfaces and an integrated, interruptible switch enable wiring for:

- In line topology with a common MAC address and IP address for both interfaces.
- Two separate networks with a common MAC address and an IP address for each interface.

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
- Modbus RTU Master/Slave (via RS-232 or RS-485)
- BACnet/IP

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 Telnet server
- 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.

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 card!

Use only the SD memory card available from WAGO (item No. 758-879/000-001) 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.



Information

Additional Information about current Software

The current software version for programming and configuring the 750-8212/0000-0100 PFC200; G2; 2ETH RS BACnet/IP, and the documentation for this can be downloaded from the website for this product under <http://www.wago.com>.

3.1 View

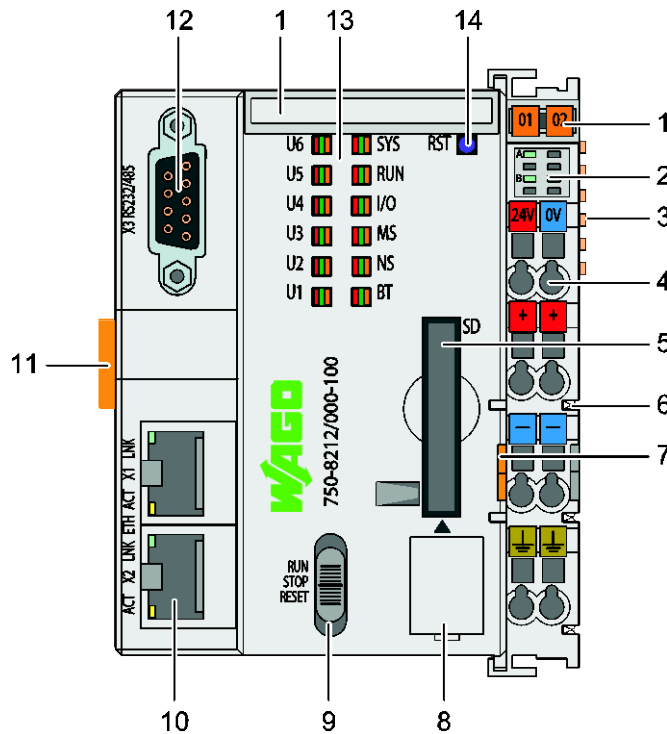


Figure 1: View

Table 3: Legend for Figure “View”

Item	Description	See section
1	Marking options (Mini WSB)	---
2	LED indicators – power supply	“Display Elements” > “Power Supply Indicating Elements”
3	Data contacts	“Connectors” > “Data Contacts/Local Bus”
4	CAGE CLAMP® connectors for power supply	“Connectors” > “CAGE CLAMP® connectors”
5	Slot for memory card	“Slot for Memory Card”
6	Power contacts for power supply of down-circuit I/O modules	“Connectors” > “Power Jumper Contacts/Field Supply”
7	Releasing strap	“Mounting” > “Inserting Devices” “Removal” > “Removing Devices”
8	Service Interface (behind the flap)	“Connectors” > “Service Interface”
9	Mode selector switch	“Operating elements” > “Operating Mode Switch”
10	ETHERNET connectors – X1, X2	“Connectors” > “Network connectors”

11	Safe locking feature	“Mounting” > “Inserting Devices” “Removal” > “Removing Devices”
12	Serial interface – X3	“Connectors” > “Communication Interface”
13	LED indicators – system	“Display Elements” > “Fieldbus/System Indicating Elements”
14	Reset button (in hole)	“Operating Elements” > “Reset Button”

3.2 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

3.2.1 Labeling Symbols

Some general information and the respective product approvals are shown in the labeling as symbols.

Table 4: Labeling Symbols

Symbol	Meaning	Description
General Symbols		
 Hansastr. 27 D-32423 Minden	Manufacturer's identification	Manufacturer name and address
	Data matrix code	One-to-one product identification by means of UII (Unique Item Identifier)
	General warning label	Read this manual carefully for safe use and proper handling
	ESD danger sign	Avoid electrostatic discharge! → See chapter "Safety Advice (Precautions)"
	WEEE label	Note on disposal → See chapter "Disposal"
Symbols of Approvals (Examples)		
	Conformity marking	Approval information → See chapter "Approvals"
	Korean Certificate	
	Ex approvals	
	Ship approvals	
	TÜV symbol	

3.2.2 Manufacturing Number

The serial number indicates the delivery status directly after production.

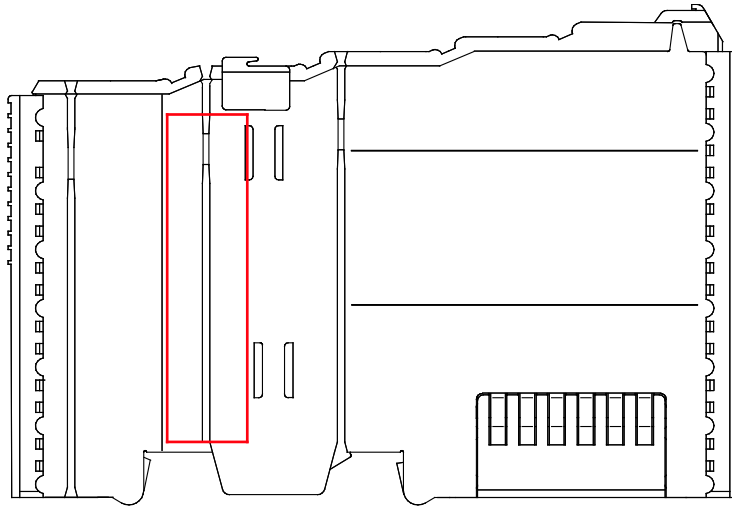


Figure 2: Marking Area for Serial Numbers

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.

In addition, the serial number is printed on the front on the cover cap of the service interface, so that it can also be read when installed.

3.2.3 Hardware Address (MAC-ID)

Each **PFC200; G2; 2ETH RS** BACnet/IP has an internationally unambiguous physical address, referred to as the MAC-ID (Media Access Control Identity).

As part of the labeling on the right side of this component, the MAC ID is printed in the block diagram.

In addition, the MAC ID is located on the paper strip with two self-adhesive peel-off strips on its left side.

The MAC ID has a fixed length of 6 bytes (48 bits) which are presented hexadecimal. The first three bytes identify the manufacturer (e.g. 00:30 DE for WAGO). The second 3 bytes comprise the unique serial number of the hardware.

3.2.4 Update Matrix

For products that can be updated, the side inscription has a prepared matrix in which the current update data can be entered in columns.

The matrix has rows to enter the “FA” production or work order number and to enter the “PD” production date and “AZ” item number.

FA	XXXXXXXXXX	
PD	WWJJ	
AZ	FWHWFL	

Figure 3: Update Matrix from 2016

Table 5: Legend for Figure “Update Matrix from 2016”

	Description
FA	Production order number, 10-digit
PD	KW = calendar week YY = year
AZ	FW = firmware index HW = hardware index FL = firmware loader index

For factory updates to a head station, the current production or work order number is also printed on the cover cap of the service interface.

The original manufacturing information on the product housing remains unchanged.

3.3 Connectors

3.3.1 Data Contacts/Local Bus

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

**Ensure that the environment is well grounded!**

The devices are equipped with electronic components that may be destroyed by electrostatic discharge. When handling the devices, ensure that the environment (persons, workplace and packing) is well grounded. Avoid touching conductive components, e.g. 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.

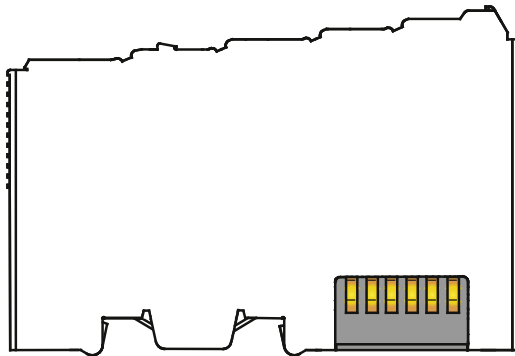


Figure 4: Data Contacts

3.3.2 Power Jumper Contacts/Field Supply

⚠ 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.

The controller 750-8212/0000-0100 is equipped with 3 self-cleaning power contacts for transferring of the field-side power supply to down-circuit I/O modules. These contacts are designed as spring contacts.

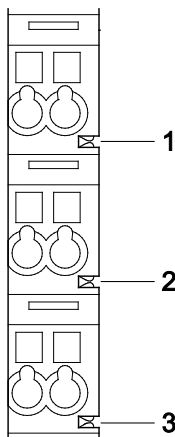


Figure 5: Power Jumper Contacts

Table 6: Legend for Figure "Power Jumper Contacts"

Contact	Type	Function
1	Spring contact	Potential transmission (U_V) for field supply
2	Spring contact	Potential transmission (0 V) for field supply
3	Spring contact	Potential transmission (ground) for field supply

NOTICE

Do not exceed maximum values via power contacts!

The maximum current that can flow through the power jumper contacts is 10 A. The power jumper contacts can be damaged and the permissible operating temperature can be exceeded by higher current values.

When configuring the system, do not exceed the permissible maximum current value. If there is a higher power requirement, you must use an additional supply module to provide the field voltage.

3.3.3 CAGE CLAMP® Connectors

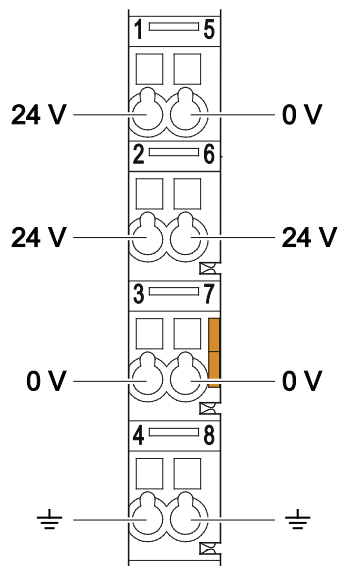


Figure 6: CAGE CLAMP® connections

Table 7: Legend for figure “CAGE CLAMP® connections”

Contact	Description	Description
1	24 V	System power supply voltage +24 V
2	+	Field-side power supply voltage U_V
3	-	Field-side power supply voltage 0 V
4	Ground	Field-side power supply voltage, ground
5	0 V	System power supply voltage 0 V
6	+	Field-side power supply voltage U_V
7	-	Field-side power supply voltage 0 V
8	Ground	Field-side power supply voltage, ground



Note

Observe supplementary power supply regulations for use in shipbuilding!
Observe supplementary power supply regulations for shipbuilding and the supply voltage in Section “Connect Devices” > ... > “Supplementary Power Supply Regulations”!

3.3.4 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”.

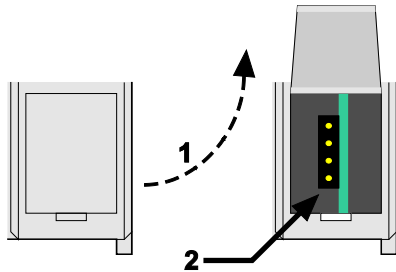


Figure 7: Service Interface (Closed and Open Flap)

Table 8: 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 numbers 750-920 and 750-923 or via the WAGO radio adapter with the item number 750-921.

3.3.5 Network Connectors

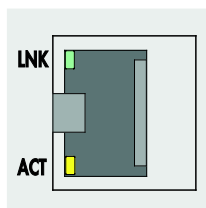


Figure 8: Network Connections – X1, X2

Table 9: 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

3.3.6 Communication Interface

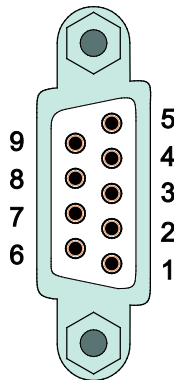


Figure 9: RS-232/RS-485 – Communication Connection – X3

Table 10: Legend for Figure “RS-232/RS-485 – Communication Connection – X3”

Contact	RS-232 (DCE)		RS-485	
	Signal	Description	Signal	Description
1	NC	Not assigned	NC	Not assigned
2	RxD (out)	Receive Data	NC	Not assigned
3	TxD (in)	Transmit Data	A (Tx/Rx+)	Transmit/receive data +
4	NC	Not assigned	NC	Not assigned
5	FB_GND	Ground	FB_GND	Ground
6	NC	Not assigned	FB_5V	Power Supply
7	RTS (in)	Request to Send	NC	Not assigned
8	CTS (out)	Clear to Send	B (Tx/Rx-)	Transmit/receive data -
9	NC	Not assigned	NC	Not assigned
Enclosure	Shield	Shielding	Shield	Shielding

If the communication interface is opened as an RS-232 interface, the controller represents data communication equipment (DCE). The RxD and CTS signals are sent to the communication partner (out), and the TxD and RTS signals are received by the communication partner (in).

NOTICE

Incorrect parameterization can damage the communication partners!

The voltage levels are -12 V and +12 V for RS-232, and -5 V and +5 V for RS-485.

If the controller interfaces differ from those of the communication partners (RS-232 <> RS-485 or RS-485 <> RS-232), this may damage the interface of the communication partner.

Therefore, always ensure that the controller interface matches those of its communication partners when configuring these items!

DC/DC converters and optocouplers in the fieldbus interface electrically isolate the fieldbus system and the electronics.

3.3.6.1 Operating as an RS-232 Interface

Depending on the device type DTE (Data Terminal Equipment, e.g., PC) or DCE (Data Communication Equipment, e.g., PFC, modem), the RS-232 signals have different data directions.

Table 11: Function of RS-232 Signals for DTE/DCE

Contact	Signal	Data Direction	
		DTE	DCE
2	RxD	Input	Output
3	TxD	Output	Input
5	FB_GND	---	---
7	RTS	Output	Input
8	CTS	Input	Output

For a DTE-to-DCE connection, the signals are connected directly (1:1).

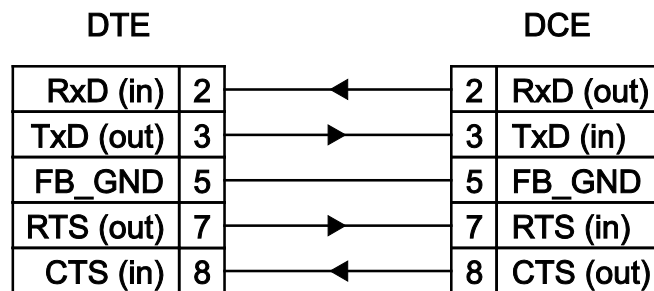


Figure 10: Termination with DTE-DCE Connection (1:1)

For a DCE-to-DCE connection, the signal connections are crossed (cross-over).

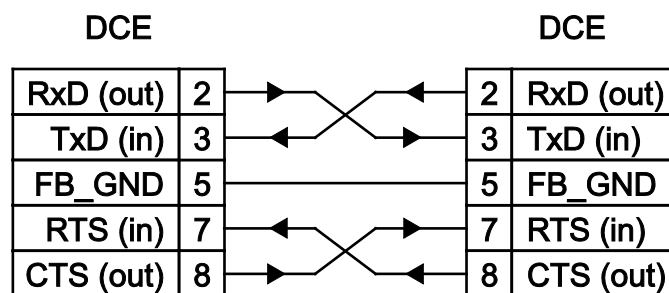


Figure 11: Termination with DCE-DCE Connection (Cross-Over)

3.3.6.2 Operating as an RS-485 Interface

To minimize reflection at the end of the line, the RS-485 line must be terminated at both ends by a cable termination. If required, one pull-up or pull-down resistor may be used. These resistors ensure a defined level on the bus when no subscriber is active, i.e., when all subscribers are in “Tri-state”.

Note



Attention — bus termination!

The RS-485 bus must be terminated at both ends!

No more than two terminations per bus segment may be used!

Terminations may not be used in stub and branch lines!

Drop cables must be kept as short as possible!

Operation without proper termination of the RS-485 network may result in transmission errors.

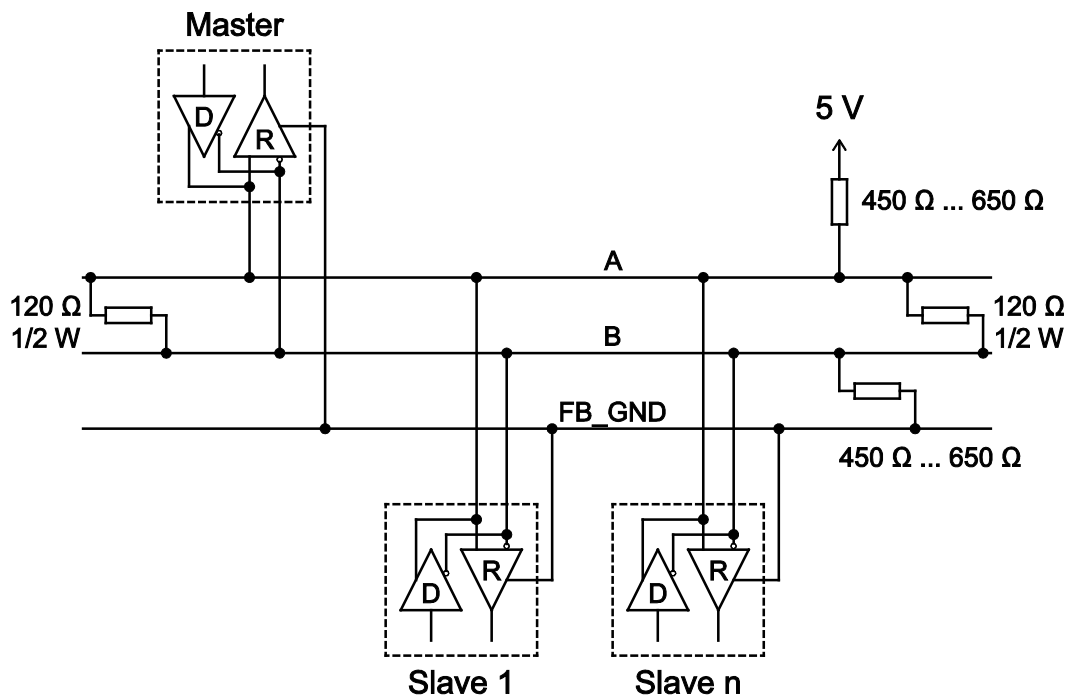


Figure 12: RS-485 Bus Termination

3.4 Display Elements

3.4.1 Power Supply Indicating Elements

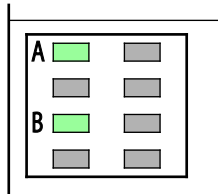


Figure 13: Power Supply Indicating Elements

Table 12: Legend for Figure “Power Supply Indicating Elements”

Designation	Color	Description
A	Green/off	Status of system power supply voltage
B	Green/off	Status of field-side power supply voltage

3.4.2 Fieldbus/System Indicating Elements













U6   SYS
 U5   RUN
 U4   I/O
 U3   MS
 U2   NS
 U1   CAN

Figure 14: Indicating Elements for System/Fieldbus

Table 13: 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
BT	Red/Green/ Orange/Off	BACnet status
U6	Red/Green/ Orange/Off	User LED 6, programmable using function blocks from the WAGO libraries to control the LEDs
U5	Red/Green/ Orange/Off	User LED 5, programmable using function blocks from the WAGO libraries to control the LEDs
U4	Red/Green/ Orange/Off	User LED 4, programmable using function blocks from the WAGO libraries to control the LEDs
U3	Red/Green/ Orange/Off	User LED 3, programmable using function blocks from the WAGO libraries to control the LEDs
U2	Red/Green/ Orange/Off	User LED 2, programmable using function blocks from the WAGO libraries to control the LEDs
U1	Red/Green/ Orange/Off	User LED 1, programmable using function blocks from the WAGO libraries to control the LEDs

3.4.3 Memory Card Indicating Elements

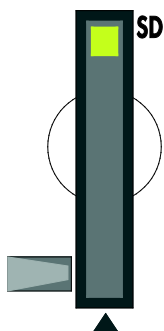


Figure 15: Indicating Elements, Memory Card Slot

Table 14: Legend for Figure “Indicating Elements, Memory Card Slot”

Designation	Color	Description
SD	Yellow/Off	Memory card status

3.4.4 Network Indicating Elements

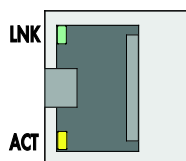


Figure 16: Indicating Elements, RJ-45 Jacks

Table 15: Legend for Figure “Indicating Elements, RJ-45 Jacks”

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

3.5 Operating Elements

3.5.1 Operating Mode Switch

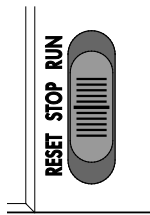


Figure 17: Mode Selector Switch

Table 16: Mode Selector Switch

Position	Actuation	Function
RUN	Latching	Normal operation <i>e!RUNTIME</i> applications running.
STOP	Latching	Stop All <i>e!RUNTIME</i> 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.

3.5.2 Reset Button

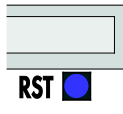


Figure 18: Reset Button

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")

3.6 Slot for Memory Card

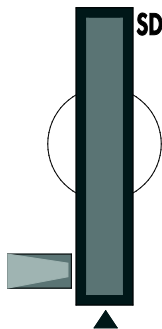


Figure 19: Slot for SD Memory Card

The slot for the SD memory card is located on the front of the housing. The memory card is locked in the enclosure by a push/push mechanism. Inserting and removing the memory card is described in the Section “Service” > “Inserting and Removing the Memory Card.”

The memory card is protected by a cover flap. The cover cap is sealable.

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 card!

Use only the SD memory card available from WAGO (item No. 758-879/000-001) 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.

3.7 Schematic Diagram

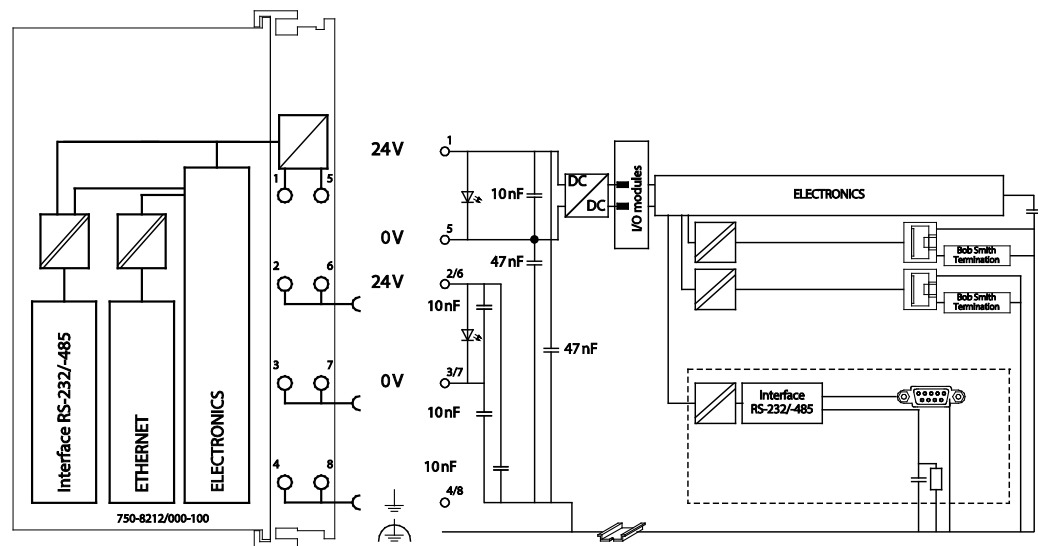


Figure 20: Schematic diagram

3.8 Technical Data

3.8.1 Mechanical Data

Table 17: Technical Data – Mechanical Data

Width	79 mm
Height (from upper edge of DIN 35 rail)	65 mm
Length	100 mm
Weight	214 g

3.8.2 System Data

Table 18: Technical Data – System Data

CPU	Cortex A8, 1 GHz
Operating System	Real-time Linux® 4.9.47-rt37 (with RT Preemption Patch)
Memory card slot	Push-push mechanism, sealable cover lid
Type of memory card	SD and SDHC up to 32 Gbytes (All guaranteed properties are valid only in connection with the WAGO 758- 879/000-001 memory card.)

3.8.3 Power Supply

Table 19: Technical Data – Power Supply

Power supply	24 VDC (-25 % ... +30 %)
Typ. input current at 24 VDC	550 mA
Max. input current at 18 VDC (24 VDC – 25 %)	761 mA
Power failure time acc. IEC 61131-2	Depending on external buffering
Total current for I/O modules (DC 5 V)	1700 mA
Isolation	500 V system/supply



Note

Buffer for system power supply!

The system power 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.

3.8.4 Clock

Table 20: Technical Data – Clock

Drift - system clock (25 °C)	20 ppm
Drift - RTC (25 °C)	3 ppm
Buffer time RTC (25 °C)	30 days

3.8.5 Programming

Table 21: Technical Data – Programming

Programming	e!COCKPIT
IEC 61131-3	LD, FBD (CFC), ST, FC
Program and data memory	60 MB (dynamically distributed)
Non-volatile memory (NVRAM, retain + flag)	128 Kbytes

3.8.6 Local Bus

Table 22: Technical Data – Local Bus

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

3.8.7 ETHERNET

Table 23: Technical Data – ETHERNET

ETHERNET	2 x RJ-45 (X1, X2) separated/switched (In “separated” mode, BACnet communication only takes place via interface X1.)
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, NTP, 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!

3.8.8 BACnet/IP

Table 24: Technical Data – BACnet/IP

BACnet/IP Protocol	ISO 16484-5: 2012; /ANSI/ASHRAE Standard 135-2012
BACnet Device Profile	BACnet-Building Controller (B-BC)
BACnet-Revision	14

Note



Interface Restriction in „Separated Mode“!

In „Separated Mode“ of the RJ-45 interfaces, BACnet communication only takes place via interface X1.

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!

3.8.9 Communication Interface

Table 25: Technical Data – Communication Interface

Interface	1 x serial interface per TIA/EIA 232 and TIA/EIA 485 (switchable), 9-pole D-sub female connector
Protocols	Modbus® RTU

3.8.10 Connection Type

Table 26: Technical Data – Field Wiring

Wire connection	CAGE CLAMP®
Cross section	0.08 mm² ... 2.5 mm², AWG 28 ... 14
Stripped lengths	8 mm ... 9 mm / 0.33 in

Table 27: Technical Data – Power Jumper Contacts

Power jumper contacts	Spring contact, self-cleaning
-----------------------	-------------------------------

Table 28: Technical Data – Data Contacts

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

3.8.11 Climatic Environmental Conditions

Table 29: 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 ≤ 25 ppm H ₂ S ≤ 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

3.8.12 Software Compatibility

Table 30: Technical Data – Software Compatibility

e!COCKPIT	(2759-101)	starting from version 1.5.1
WAGO-I/O-CHECK	(759-302)	starting from version 3.20.01(01)
WAGO Ethernet Settings	(759-316)	starting from version 6.10.04.10
WAGOupload	(www.wago.com)	starting from version 1.10.0.0
WAGO BACnet Configurator	(759-321)	starting from version 1.12.0.0

3.9 Approvals



Information

More information about approvals.

Detailed references to the approvals are listed in the document “Overview Approvals **WAGO I/O SYSTEM 750**”, which you can find via the internet under: www.wago.com → DOWNLOADS → Documentation → System Description.

The following approvals have been granted to the “PFC200; G2; 2ETH RS BACnet/IP” controller (750-8212/0000-0100):



Conformity Marking



Korea Certification

MSIP-REM-W43-PFC750

The following approvals are pending for 750-8212/0000-0100 controller:



Ordinary
Locations

UL61010-2-201

The following Ex approvals have been granted to the “PFC200; G2; 2ETH RS BACnet/IP” controller (750-8212/0000-0100):



TÜV 14 ATEX 148929 X

II 3 G Ex ec IIC T4 Gc

IECEx TUN 14.0035 X

Ex ec IIC T4 Gc

The following Ex approvals are pending for the “PFC200; G2; 2ETH RS BACnet/IP” controller (750-8212/0000-0100) described in this document:



Hazardous
Locations

UL 121201 for Use in Hazardous Locations
CI I Div 2

The following ship approvals are pending for the “PFC200; G2; 2ETH RS BACnet/IP” controller (750-8212/0000-0100) described in this document:



ABS (American Bureau of Shipping)



DNV GL

[Temperature: B, Humidity: B, Vibration: B, EMC: B, Enclosure: (*)]

(*) Required protection according to the rules shall be provided upon installation on board.



Information

For more information about the ship approvals:

Note the "Supplementary Power Supply Regulations" section for the ship approvals.

3.10 Standards and Guidelines

The “PFC200; G2; 2ETH RS BACnet/IP” controller (750-8212/0000-0100) fulfills the following safety standards:

Electrical Equipment For UL61010-1
Measurement, Control, and Laboratory
Use; Part 1: General Requirements

Safety requirements for electrical UL61010-2-201
equipment for measurement,
control and laboratory use
Part 2-201: Particular requirements
for control equipment


The “PFC200; G2; 2ETH RS BACnet/IP” controller (750-8212/0000-0100) fulfills the following EMC standards:

EMC CE-Immunity to interference EN 61000-6-2

EMC CE-Emission of interference EN 61000-6-3

The following BACnet approvals have been granted to the respective software versions (SW):

Table 31: BACnet Approvals

BACnet Approvals	750-8212/000-100
BACnet conformance test acc. ISO 16484-5:2017	Pending *
 BTL Certification	Pending *
AMEV attestation AMEV Profile AS-B	Pending *

* Status as of 6/2019
Further certifications are currently in preparation.

3.11 BACnet-Building-Controller (B-BC)

The 750-8212/0000-0100 WAGO PFC200; G2; 2ETH RS BACnet/IP represents the device profile of the BACnet Building Controllers (B-BC). As such, the controller serves as a programmable automation system that can take over a multitude of different building automation and control tasks.

The BACnet Standard 135-2012 describes six BACnet device profiles. Any device that implements all the required BACnet capabilities for a particular device type and interoperability area may claim to be a device of that particular device profile. Devices may also provide additional capabilities. All supported capabilities of the controller must be indicated in the protocol implementation confirmation (PICS). This is a document that represents and compares the capabilities of the device.



Information

Additional Information

You can download the appropriate PICS document on the product page of your controller at: www.wago.com.

As a B-BC the controller „PFC200; G2; 2ETH RS BACnet/IP“ (750-8212/0000-0100) supports the following parameters:

Data Sharing

- Ability to provide the values of any of its BACnet objects
- Ability to retrieve the values of BACnet objects from other devices
- Ability to allow modification of some or all of its BACnet objects by an-other device
- Ability to modify some BACnet objects in other devices

Alarm and Event Management

- Generation of alarm/event notifications and the ability to direct them to recipients
- Maintain a list of unacknowledged alarms/events
- Notifying other recipients that the acknowledgment has been received
- Adjustment of alarm and event parameters, scheduling
- Ability to schedule output actions, both in the local device and in other devices, both binary and analog, based on date and time

Trending

- Collection and delivery of (time, value) pairs

Device und Network Management

- Ability to respond to queries about its status
- Ability to respond to requests for information about any of its objects
- Ability to respond to communication control messages
- Ability to synchronize its internal clock upon request
- Ability to perform re-initialization upon request
- Ability to upload its configuration and allow it to be subsequently restored

3.11.1

BIBBs (BACnet Interoperability Building Blocks)

The following table shows the minimum requirement of the BACnet features ("BACnet Interoperability Building Blocks" - BIBBs) for the B-BC in general and the additionally implemented BIBBs in the controller PFC200; G2; 2ETH RS BACnet/IP.

Table 32: BIBBs of the B-BC

IOB	BIBBs of the B-BC ¹ (Minimum requirements)	Additional BIBBs of the PFC200; G2; 2ETH RS BACnet/IP ²
Data Sharing	DS-RP-A,B DS-RPM-A,B DS-WP-A,B DS-WPM-B	DS-COV-A,B DS-COVP-B
Alarm and Event Management	AE-N-I-B AE-ACK-B AE-INFO-B AE-ESUM-B	AE-N-E-B AE-ASUM-B AE-EL-I-B
Scheduling	SCHED-E-B	SCHED-I-B
Trending	T-VMT-I-B T-ATR-B	T-VMT-E-B T-VMMV-I-B T-VMMV-E-B T-AMVR-B
Device & Network Management	DM-DDB-A,B DM-DOB-B DM-DCC-B DM-TS-B or DM-UTC-B DM-RD-B DM-BR-B	DM-R-A DM-R-B DM-LM-B DM-OCD-B

¹ As of BACnet Standard 135-2012² As of 08/2019 (For currently supported BIBBs of the PFC200; G2; 2ETH RS BACnet/IP, please refer to the "PICS" document at <http://www.wago.com> in the Documentation area.

3.11.2 Data Sharing BIBBs

These BIBBs prescribe the BACnet capabilities required to interoperably perform the data sharing functions.

Data Sharing - ReadProperty-A (DS-RP-A)

The A device is a user of data from device B.

BACnet Service	Requests	Execute
ReadProperty	x	

Data Sharing - ReadProperty-B (DS-RP-B)

The B device is a provider of data to device A.

BACnet Service	Requests	Execute
ReadProperty		x

Data Sharing-ReadPropertyMultiple-A (DS-RPM-A)

The A device is a user of data from device B and requests multiple values at one time.

BACnet Service	Requests	Execute
ReadPropertyMultiple	x	

Data Sharing-ReadPropertyMultiple-B (DS-RPM-B)

The B device is a provider of data to device A and returns multiple values at one time.

BACnet Service	Requests	Execute
ReadPropertyMultiple		x

Data Sharing-WriteProperty-A (DS-WP-A)

The A device sets a value in device B.

BACnet Service	Requests	Execute
WriteProperty	x	

Data Sharing-WriteProperty-B (DS-WP-B)

The B device allows a value to be changed by device A.

BACnet Service	Requests	Execute
WriteProperty		x

Data Sharing-WritePropertyMultiple-B (DS-WPM-B)

The B device allows multiple values to be changed by device A at one time.

BACnet Service	Requests	Execute
WritePropertyMultiple		x

BIBB - Data Sharing-COV-A (DS-COV-A)

Device A is a user of the COV data from device B.

BACnet Service	Requests	Execute
SubscribeCOV	x	
ConfirmedCOVNotification		x
UnconfirmedCOVNotification		x

The support of subscriptions with limited lifetime is necessary; the support of subscriptions with unlimited lifetime is optional.

Data Sharing-COV-B (DS-COV-B)

Device B is a provider of COV data for device A.

BACnet Service	Requests	Execute
SubscribeCOV		x
ConfirmedCOVNotification	x	
UnconfirmedCOVNotification	x	

Devices that comply with DS-COV-B must support at least five simultaneous subscriptions. The support of subscriptions with a limited lifetime is necessary; the support of subscriptions with an unlimited lifetime is optional.

Data Sharing-COVP-B (DS-COVP-B)

Device B is a provider of COV data for device A.

BACnet Service	Requests	Execute
SubscribeCOVProperty		x
ConfirmedCOVNotification	x	
UnconfirmedCOVNotification	x	

Devices that comply with DS-COV-B must support at least five simultaneous subscriptions. The support of subscriptions with a limited lifetime is necessary; the support of subscriptions with an unlimited lifetime is optional.

3.11.3 Alarm and Event Management BIBBs

These BIBBs prescribe the BACnet capabilities required to interoperably perform the alarm and event management functions.

Alarm and Event-Notification Internal-B (AE-N-I-B)

Device B generates notifications about alarms and other events.

BACnet Service	Requests	Execute
ConfirmedEventNotification	x	
UnconfirmedEventNotification	x	

Devices claiming conformance to AE-N-I-B must also support either Intrinsic or Algorithmic reporting. Any device that supports the generation of event notifications that require operator acknowledgment must support AE-ACK-B.

Alarm and Event-Notification External-B (AE-N-E-B)

Device B contains an Event Enrollment object that monitors values in another device. Device B is capable of generating event notifications for alarm conditions based on value(s) in another device. Devices conforming to the BIBB shall confirm to DS-RP-A, AE-N-I-B, and shall support at least 1 Event Enrollment object. With an Object_Property_Reference property that supports references to properties in objects contained in other devices. Any devices that supports the generation of event notifications that require operator acknowledgment shall support AE-ACK-B and AE-INFO-B. Any devices that supports the generation of TO-FAULT or TO-OFFNORMAL event notifications shall support AE-INFO-B.

Devices that only support Event Enrollment objects that only support generation of CHANGE_OF_LIFE_SAFETY and/or BUFFER_READY notifications shall not claim support for this BIBB.

Alarm and Event-ACK-B (AE-ACK-B)

Device B processes acknowledgments of previously transmitted alarm/event notifications.

BACnet Service	Requests	Execute
AcknowledgeAlarm		x

To support this BIBB the device must also support acknowledgeable alarms.

Alarm and Event-Information-B (AE-INFO-B)

Device B provides event information to device A

BACnet Service	Requests	Execute
GetEventInformation		x

Alarm and Event-Alarm Summary-B (AE-ASUM-B)

BACnet Service	Requests	Execute
GetAlarmSummary		x

Device B provides summaries of alarms to device A.

Alarm and Event-Enrollment Summary-B (AE-ESUM-B)

Device B provides event enrollments to device A.

BACnet Service	Requests	Execute
GetEnrollmentSummary		x

Alarm and Event Management-Event Log Internal-B (AE-EL-I-B)

Device B collects the event notifications in an internal buffer. Each device claiming conformance to AE-EL-I-B must be able to support at least one Event Log object.

BACnet Service	Requests	Execute
ReadRange		x

3.11.4 Scheduling BIBBs

These BIBBs prescribe the BACnet capabilities required to interoperably perform the scheduling functions.

Scheduling-Internal-B (SCHED-I-B)

Device B indicates time and data for the scheduling of values of a certain property of certain objects of the device. Each SCHED-I-B compliant device also has at least one Calendar and Schedule Object for the support of the BIBBs DS-RP-B and DS-WP-B. SCHED-I-B compliant devices must also support DM-TS-B and DM-UTC-B.

The Schedule Object must support at least six entries per day. The property List_Of_Object_Property_Reference must support at least one entry. The Schedule Object must support a non-empty property Exception_Schedule. The property Priority_For_Writing of the Schedule Object must be writable.

Scheduling-External-B (SCHED-E-B)

The B device provides date and time scheduling of the values of specific properties of specific objects in other devices. Devices claiming conformance to SCHED-E-B shall also support SCHED-I-B and DS-WP-A. The List_Of_Object_Property_References property shall support references to objects in external devices.

3.11.5 Trending BIBBs

These BIBBs prescribe the BACnet capabilities required to interoperably perform the trend value processing.

Trending-Viewing and Modifying Trends Internal-B (T-VMT-I-B)

The B device collects the trend log data records in an internal buffer. Each device-claiming conformance to T-VMT-I-B must be able to support at least one Trend Log object.

BACnet Service	Requests	Execute
ReadRange		x

Trending-Automated Trend Retrieval-B (T-ATR-B)

The B device notifies the A device that a trending buffer has acquired a predetermined number of data samples using the BUFFER_READY event algorithm either intrinsically in the Trend Log object or algorithmically using an Event Enrollment object.

BACnet Service	Requests	Execute
ConfirmedEventNotification	x	
ReadRange		x

T-ATR-B compliant devices must support the Trend Log Object.

Trending-Viewing and Modifying Trends External-B (T-VMT-E-B)

The B device is capable of trending properties of objects contained in other devices. The B device shall support T-VMT-I-B and DS-RP-A. The Log_Interval and Log_DeviceObjectProperty properties must be writable.

The Trend Log objects must be capable of trending REAL, Unsigned, INTEGER, BOOLEAN, Bit String, Enumerated and NULL values.

Trending-Viewing and Modifying Multiple Values Internal-B (T-VMMV-I-B)

The device B collects the multiple-data log records in an internal buffer. Each device claiming conformance to T-VMMV-I-B shall be able to support at least one Trend Log Multiple object.

BACnet Service	Requests	Execute
ReadRange		x

Trending-Viewing and Modifying Multiple Values External-B (T-VMMV-E-B)

The B device is capable of logging multiple properties of multiple objects contained in other devices. The B device shall support T-VMMV-I-B and DS-RPM-A. The Log_Interval and Log_DeviceObjectProperty properties shall be writable.

Trending-Automated Multiple Value Retrieval-B (T-AMVR-B)

The B device notifies the A device that a Trend Log Multiple object's buffer has acquired a predetermined number of data samples using the BUFFER_READY event algorithm either intrinsically in the Trend Log Multiple object or algorithmically using an Event Enrollment object.

BACnet Service	Requests	Execute
ConfirmedEventNotification	x	
UnconfirmedEventNotification	x	
ReadRange		x

Devices claiming conformance to T-AMVR-B shall support the Trend Log Multiple object.

3.11.6 Device- und Network-Management-BIBBs

These Device Management BIBBs prescribe the BACnet capabilities required to interoperably perform the device management functions. The network management BIBBs prescribe the BACnet capabilities required to interoperably perform network management functions.

Device Management-Dynamic Device Binding-A (DM-DDB-A)

The A device searches for information on the device properties of other devices and evaluates their notices.

BACnet Service	Requests	Execute
Who-Is	x	
I-Am		x

Device Management-Dynamic Device Binding-B (DM-DDB-B)

The B device provides information about its device properties and responds to requests to identify itself.

BACnet Service	Requests	Execute
Who-Is		x
I-Am	x	

Device Management-Dynamic Object Binding-B (DM-DOB-B)

The B device provides address information about its objects upon request.

BACnet Service	Requests	Execute
Who-Has		x
I-Have	x	

Device Management-DeviceCommunicationControl-B (DM-DCC-B)

The B device responds to communication control exercised by the A device.

BACnet Service	Requests	Execute
DeviceCommunicationControl		x

Support for requests of a limited duration is required, and support for requests of

an indefinite duration is optional.

Device Management-Restart-A (DM-R-A)

The A device processes restart notifications.

BACnet Service	Requests	Execute
UnconfirmedCOVNotification		x

Device Management-Restart-B (DM-R-B)

The B device informs the A device(s) each time it restarts.

BACnet Service	Requests	Execute
UnconfirmedCOVNotification	x	

Devices claiming conformance to DM-R-B shall support the Last_Restart_Reason, Restart_Notification_Recipients, and Time_Of_Device_Restart properties of the Device object.

Device Management-TimeSynchronization-B (DM-TS-B)

The B device interprets time synchronization messages from the A device.

BACnet Service	Requests	Execute
TimeSynchronization		x

DM-TS-B compliant devices must support the Local_Time and Local_Date properties of the Device object.

Device Management-UTCTimeSynchronization-B (DM-UTC-B)

The B device interprets time synchronization messages from the A device.

BACnet Service	Requests	Execute
UTCTimeSynchronization		x

DM-TS-B compliant devices must support the Local_Time, Local_Date, UTC_Offset, and Daylight_Savings_Status properties of the Device object.

Device Management-ReinitializeDevice-B (DM-RD-B)

The B device performs reinitialization requests from the A device. The optional password field shall be supported.

BACnet Service	Requests	Execute
ReinitializeDevice		x

Device Management-Backup and Restore-B (DM-BR-B)

The B device provides its configuration file to the A device and allows the A device to write this file to recover its configuration in the event of a failure.

BACnet Service	Requests	Execute
AtomicReadFile		x
AtomicWriteFile		x
ReinitializeDevice		x

DM-BR-B compliant devices must support the features of device B. Once a Restore procedure has been initiated on the device, the Read_Only property of configuration File objects shall contain the value FALSE and the File_Size property of the configuration File objects shall be writable if the size of the configuration file can change based on the device's configuration.

If the configuration file objects are not guaranteed to exist once a Restore procedure has been initiated, then the device must support execution of the CreateObject service.

Device Management-List Manipulation-B (DM-LM-B)

The B device responds to requests to add or remove list elements.

BACnet Service	Requests	Execute
AddListElement		x
RemoveListElement		x

Device Management-Object Creation and Deletion-B (DM-OCD-B)

The B device creates and deletes object instances based on requests from the A device. The object types whose dynamic creation and deletion is supported shall be enumerated in the Standard Object Types Supported section of the device B's PICS.

BACnet Service	Requests	Execute
CreateObject		x
DeleteObject		x

4 Function Description

4.1 Network

4.1.1 Interface Configuration

The ETHERNET X1 and X2 interfaces of the controller are connected with an internal 3-port switch, in which the third port is connected to the CPU. Interfaces X1 and X2 can either be operated in Switch mode or as separate network interfaces. The switching can be performed during the runtime. The Switch mode is activated by default and during initial startup. The "Configuration mode" is set to "DHCP."

For interface X1, a fixed IP address can be set temporarily ("Fix IP Address" mode). The setting is carried out with the Reset button (see Section "Commissioning" > ... > "Temporarily Setting a Fixed IP Address").

Setting a fixed IP address has no effect on the mode previously set.

4.1.1.1 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.

4.1.1.2 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.



Note

Interface Restriction in „Separated Mode“!

In „Separated Mode“ of the RJ-45 interfaces, BACnet communication only takes place via interface X1.

4.1.2 Network Security

4.1.2.1 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.

4.1.2.1.1 Services and Users

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

Service	Users					
	WBM		Linux®			SNMP
	admin	user	root	admin	user	
Web Based Management (WBM)	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

4.1.2.1.2 WBM User Group

WBM has its own user administration system. The users in this system are isolated from the other user groups in the system for security reasons.

Detailed information about this is given in the Section “WBM User Administration”.

Table 33: WBM Users

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



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.

4.1.2.1.3 Linux® User Group

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

The passwords for these users must be configured through a terminal connection via SSH/RS-232.

Table 34: 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



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.

4.1.2.1.4 SNMP User Group

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

4.1.2.2 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.

4.1.2.2.1 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”.

4.1.2.3 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”).

4.1.3 Network Configuration

4.1.3.1 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. If there are multiple network interfaces with DHCP, the last received host name is valid. 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.

4.1.4 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.

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:

If the value "default" is entered in the "Destination Address" field, a default gateway, also called a default route, is defined. The value "0.0.0.0" must then be set in the "Destination Mask" field.

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.

If the IP address of the gateway is outside the IP address space that the controller can reach, the associated route is not enabled.

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. The default value for the metric is 20. Besides the manually configurable routes, default gateways can also be set via DHCP replies. All default gateways transferred via DHCP are assigned a permanent metric value of 10.

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, "Routing enabled entirely" must be enabled in the "General Routing Configuration" 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

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.

4.1.5 Network Services

4.1.5.1 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 (X1, X2).

The Hostname and Domain parameters are stored according to the LIFO principle (Last In First Out). The settings from the last DHCP offer received are always used.

The DNS and NTP Server parameters are stored centrally for global use. All transmitted parameters are saved.

4.1.5.2 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 35: 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.

4.1.5.3 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.

4.1.6 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.

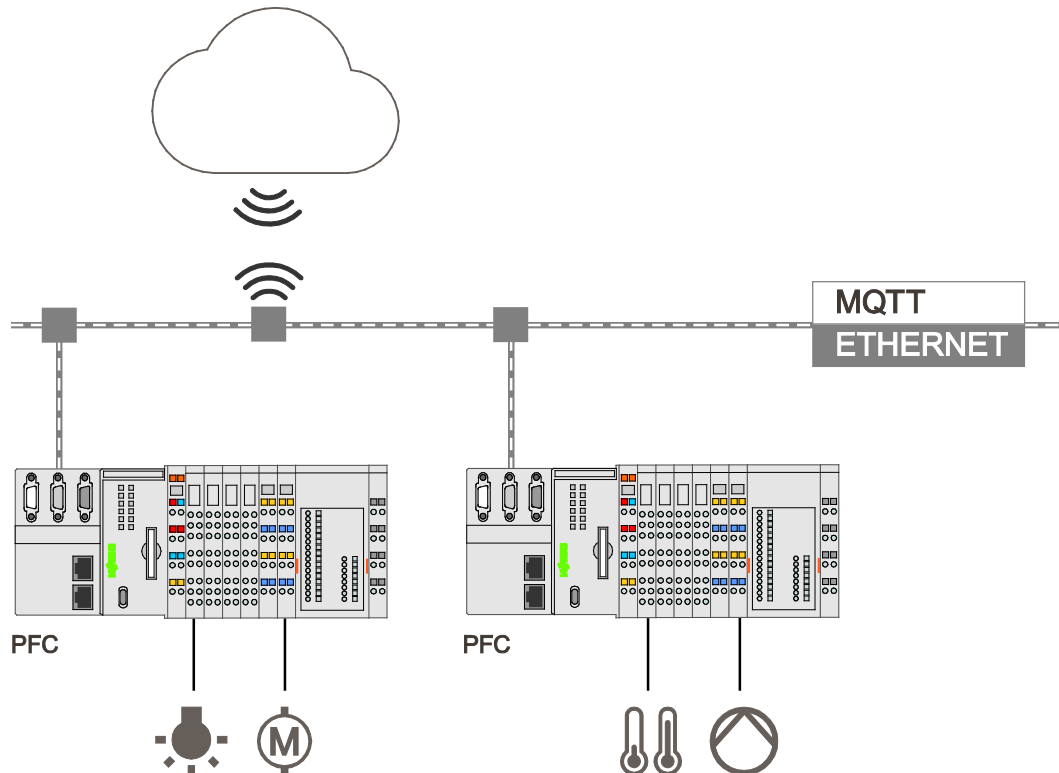


Figure 21: Connecting the Controller to a Cloud Service (Example)

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.

4.1.6.1 Components of the Cloud Connectivity Software Package

Table 36: 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.

4.2 Memory Card Function



Note

Only use recommended memory card!

Use only the SD memory card available from WAGO (item No. 758-879/000-001) 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.



Note

Deactivate write protection!

In order to be able to write data to the memory card, you must deactivate the write protection using the small push switch for the write protection setting. This switch is on one of the long sides of the memory card.

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.

4.2.1 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.



Note

FAT formatting for BACnet data!

Format the memory card as FAT to save recorded trend log, event log, or persistent BACnet data to the memory card.

4.2.2 Data Backup

The controller has a backup function and a restore function.

The necessary settings can be made and the functions can be executed via the WBM pages or via the CBM "Backup" and "Restore" menus.

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 ("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.

4.2.2.1 BACnet Data Assurance

The BACnet data is an exception for data backup.

BACnet data is neither saved during backup via the WBM / CBM, nor is the BACnet configuration restored via restore in the WBM / CBM.

For this reason, the described backup of the CODESYS projects, device settings and the controller operating system via the backup and restore function for the BACnet data does not apply.

For the storage of BACnet persistence data, trend log and event log data, special settings are possible on the WBM pages that are available for BACnet. These settings are only relevant for the BACnet data at this point and are only executed from there.

This also allows the deletion of persistence data, the BACnet upload by means of the "Override.xml" file and resetting to the BACnet factory setting, as well as the exporting and saving of the BACnet data to an inserted memory card.

If the option for saving to SD card is selected and the memory card is removed during operation, the 'BT'-LED signals this behavior.

If the SD card is dragged while the storage is active, the persistence data controller automatically switches the location to the flash. However, it can still lead to data loss.

For the trend or eventlog data, removing the SD card causes logging to be interrupted.



Information

Further information about the settings for the BACnet data!

Further information on the possible settings for the BACnet data can be found on the WBM pages available for BACnet in the chapter "Commissioning" >> "Configuring" >> "Configuring using Web-Based Management" >> "Page "Configuration of General BACnet" and subsequent.



Information

Further information on the evaluation of the 'BT'-LED!

Details on the evaluation of the 'BT' LED signaling can be found in the chapter "Diagnostics" >> "System/Fieldbus Display Elements".

4.2.2.2 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 via the WBM page "Firmware Backup" or the CBM menu "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.

4.2.2.3 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 via the WBM page "Firmware Restore" or the CBM menu "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 "Boot project location" setting on the "General PLC Runtime Configuration Web" page of the WBM determines whether the boot project of the internal drive or the memory card is loaded.

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.

4.2.3 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.

4.2.4 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.

4.2.5 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.

Some conditions must be met before moving the directory.

- A running IEC-61131 application must be stopped and the device restored to its initial state using the "Reset" function. Any boot project is deleted.
- 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.

Only when the two conditions are met can the "Home directory on memory card enabled" checkbox be selected from the WBM on the "PLC Runtime" page.

Press the **[Submit]** button to apply the settings, which take 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 booted 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.

4.2.6 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 37: 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

5 Mounting

5.1 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

5.2 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.

5.3 Mounting onto Carrier Rail

5.3.1 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).

5.3.2 WAGO DIN Rails

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

Table 38: 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.

5.4 Spacing

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

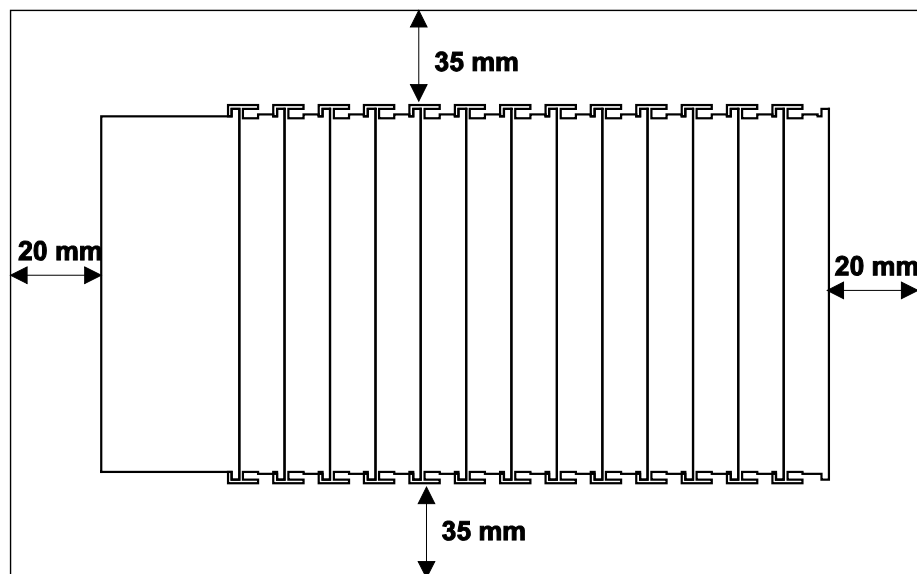


Figure 22: Spacing

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

5.5 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 (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.

5.6 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.

5.6.1 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.

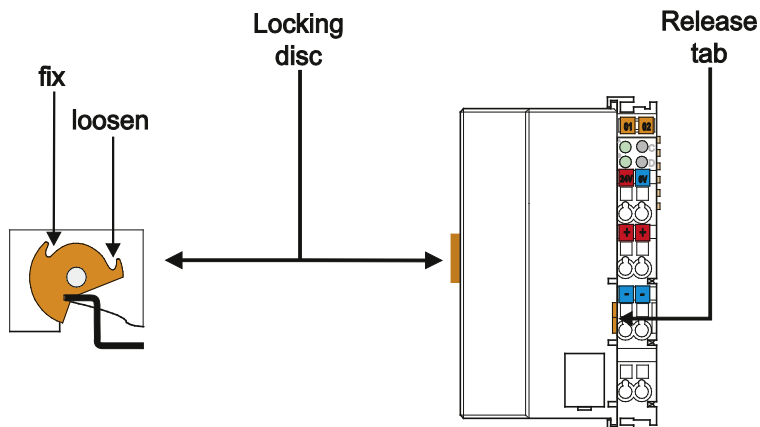


Figure 23: Release Tab of Controller

6 Connect Devices

6.1 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.

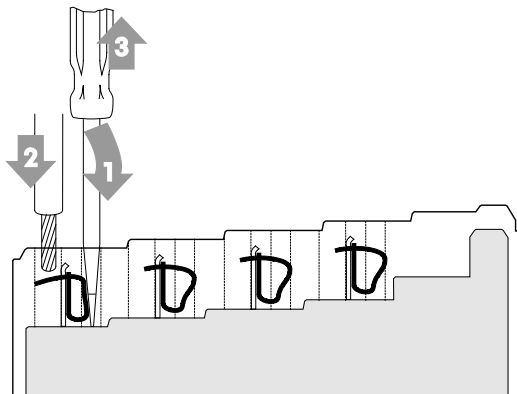


Figure 24: Connecting a Conductor to a CAGE CLAMP®

6.2 Power Supply Concept

6.2.1 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 protection 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.

6.2.2 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 39: 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.

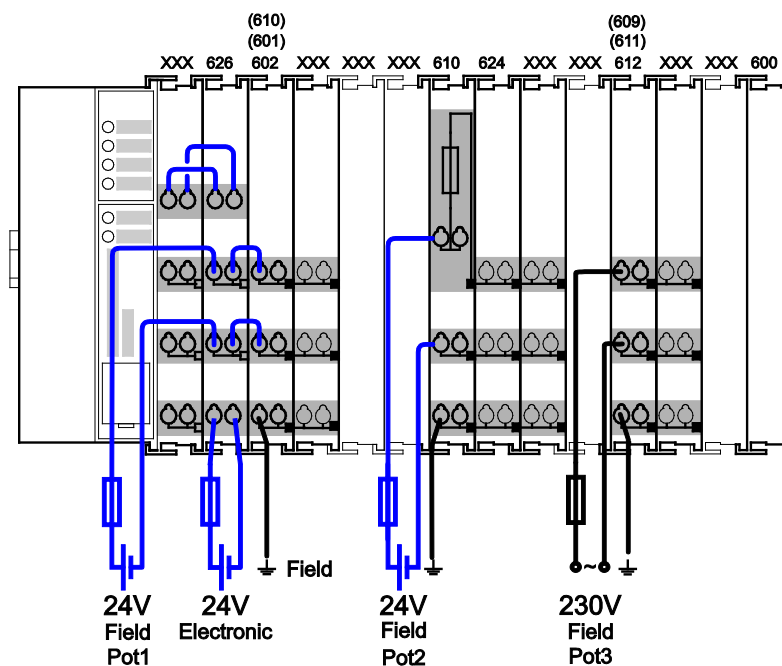


Figure 25: Power Supply Concept

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.

7 Commissioning

7.1 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 (750-600) (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”).

After the system startup is complete, the BACnet fieldbus status is indicated by the BT LED.

7.2 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.

7.3 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 40: 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 (WBM, WAGO ETHERNET Settings or CBM – 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 mask 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 41: Network Mask 255.255.255.0

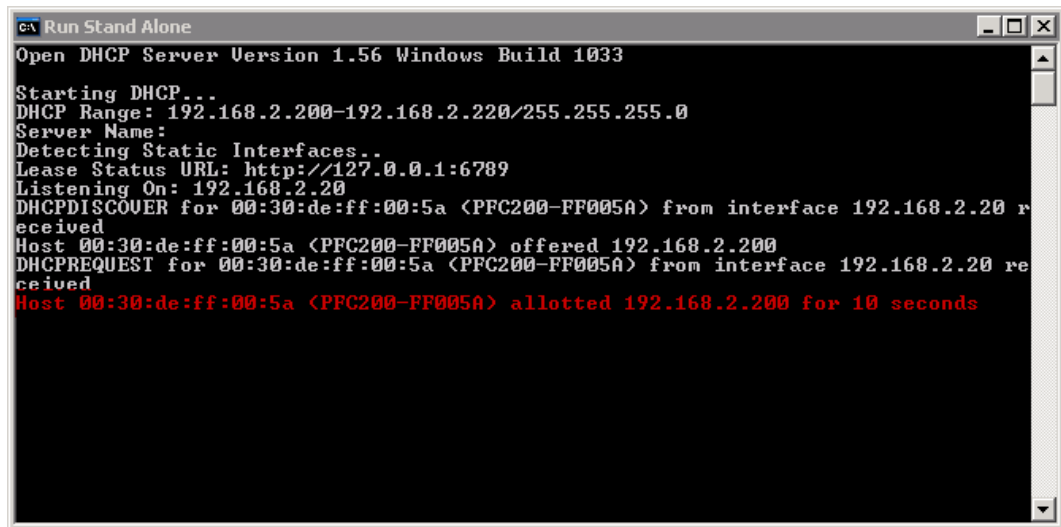
Host PC	Subnet Address Range for the Controller
192.168.1.2	192.168.1.1 or 192.168.1.3 ... 192.168.1.254

7.3.1 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.



```
Run Stand Alone
Open DHCP Server Version 1.56 Windows Build 1033

Starting DHCP...
DHCP Range: 192.168.2.200-192.168.2.220/255.255.255.0
Server Name:
Detecting Static Interfaces..
Lease Status URL: http://127.0.0.1:6789
Listening On: 192.168.2.20
DHCPDISCOVER for 00:30:de:ff:00:5a <PFC200-FF005A> from interface 192.168.2.20 received
Host 00:30:de:ff:00:5a <PFC200-FF005A> offered 192.168.2.200
DHCPPREREQUEST for 00:30:de:ff:00:5a <PFC200-FF005A> from interface 192.168.2.20 received
Host 00:30:de:ff:00:5a <PFC200-FF005A> allotted 192.168.2.200 for 10 seconds
```

Figure 26: “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”.

7.3.2 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.

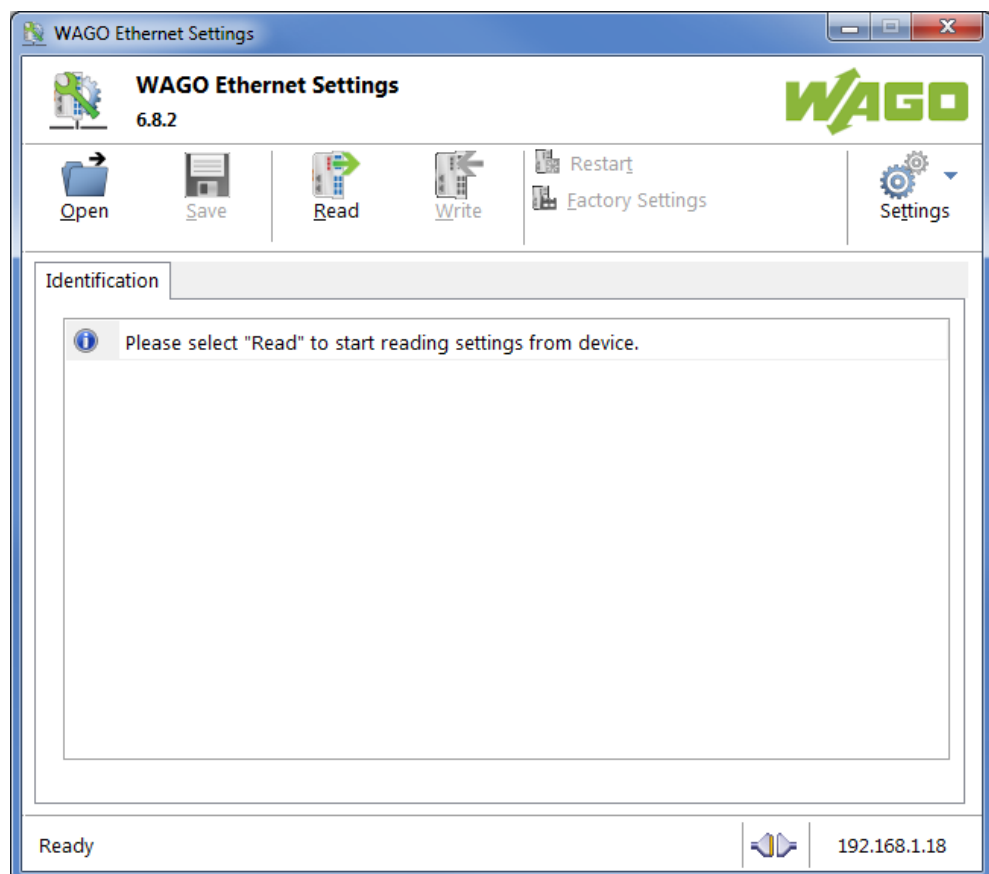


Figure 27: “WAGO Ethernet Settings” – Starting Screen (Example)

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

6. Select the “Network” tab:

Parameter	Edit	Currently used
Address Source	Static Configuration	Static Configuration
IP address	192.168.1.18	192.168.1.18
Subnet Mask	255.255.255.0	255.255.255.0
Gateway	0.0.0.0	0.0.0.0
Preferred DNS-Server	0.0.0.0	0.0.0.0
Alternative DNS-Server	0.0.0.0	0.0.0.0
Time Server	0.0.0.0	0.0.0.0
Hostname		PFC200-400E6F
Domain name	localdomain.lan	localdomain.lan

Interface X1
Interface X2
Run WBM

Interfaces
☐ Switched
☒ Separated

Figure 28: “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.

7.3.3 Temporarily Setting a Fixed IP Address

This procedure temporarily sets the IP address for the X1 interface to the fixed address "192.168.1.17".

When the switch is enabled, the fixed address is also used for interface X2.

When the switch is disabled, the original address setting for interface X2 is not changed.

No reset is performed.

To make this setting, 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.

To cancel this setting, proceed as follows:

- Perform a software reset or
- Switch off the controller and then switch it back on.

7.4 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.

```
C:\WINDOWS\system32\cmd.exe
U:\>ping 192.168.1.17

Ping wird ausgeführt für 192.168.1.17 mit 32 Bytes Daten:

Antwort von 192.168.1.17: Bytes=32 Zeit=1ms TTL=64
Antwort von 192.168.1.17: Bytes=32 Zeit<1ms TTL=64
Antwort von 192.168.1.17: Bytes=32 Zeit<1ms TTL=64
Antwort von 192.168.1.17: Bytes=32 Zeit<1ms TTL=64

Ping-Statistik für 192.168.1.17:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
    Ca. Zeitangaben in Millisek.:
        Minimum = 0ms, Maximum = 1ms, Mittelwert = 0ms

U:\>
```

Figure 29: Example of a Function Test

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

7.5 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.
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.
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.

7.6 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.

7.7 Initiating Reset Functions

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

7.7.1 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.

7.7.2 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.

7.7.3 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.



Note

The reset functions do not affect the BACnet data!

Please note that the BACnet data are not affected when reset functions are triggered by means of the operating mode switch and reset button (RST).

To reset the BACnet data to the factory default, open the WBM and select on the WBM page "Configuration of General BACnet" → Group "BACnet General Parameter" the parameter "Reset all BACnet Data and Settings to Default".

Here you can also delete all persistence data with the parameter "Delete Persistence Data".

7.8 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.”

Note

**BACnet configuration is not provided via CBM!**

Note that the CBM for the BACnet configuration does not have any menus, because a configuration of BACnet is not provided in the CBM.

Use instead the associated WBM pages for the BACnet configuration.

7.8.1 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. To access the pages, enter “https://” followed by the controller’s IP address and “/wbm” in the address line of your web browser, e.g., “https://192.168.1.17/wbm.”
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”).

If you have installed a DHCP server on your PC and would like to access WBM through DHCP, use the other interface. You can find detailed information about this in the section “Assigning an IP Address Using DHCP.”

Note



Displaying the Controller Start Page

If the controller does not display the start page, ensure that your web browser settings permit the bypassing of the proxy server for local addresses. Also check whether your PC is located in the same subnet as the controller.

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.

Some pages of the WBM are accessible only for certain users. They are only displayed if you have logged into the WBM. You can access the login form via the “Login” link. Pages which cannot be accessed with your current user name are already grayed out in the navigation. You can nevertheless select the entries in the navigation bar and are then routed directly to the login form.

As soon as you have logged in, your current user name is displayed in the header of the WBM. By clicking the “Logout” link you can log out again and then log in again with a different user name. When using the WBM without logging in, you are granted “Guest” access rights.

You must be logged into the WBM in order to have write or read access to (most) parameters. This is checked with every access to the device.

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.

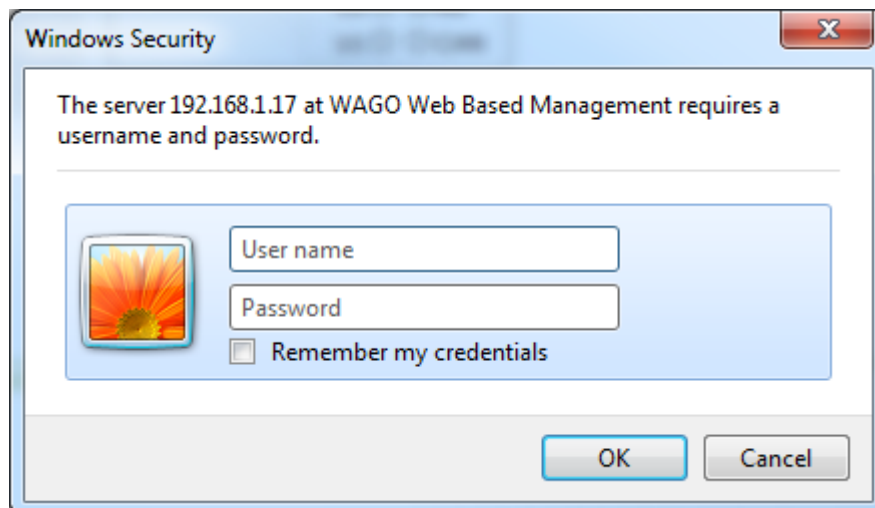


Figure 30: Entering Authentication

7.8.1.1 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

The standard passwords are documented in these instructions and thus 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.

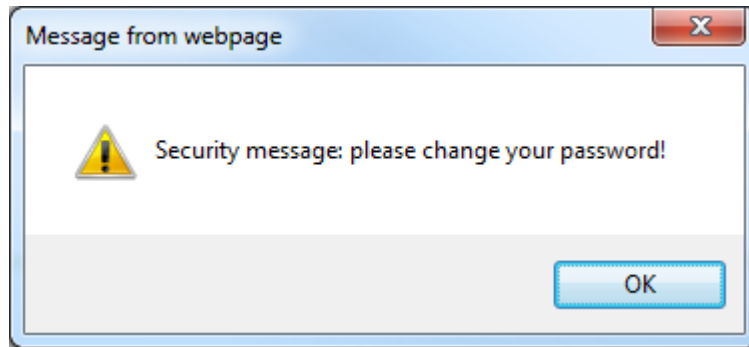


Figure 31: Password Reminder

Table 42: User Settings in the Default State

Users	Password
user	user
admin	wago



Note

Observe access rights

Users in WBM are authorized exclusively for access to websites. User administration for controller applications is configured separately.

Access to the WBM pages is as follows:

Table 43: Access Rights for WBM Pages

Navigation	WBM page	User
Information	Status Information	guest
PLC Runtime		
– Information	PLC Runtime Information	guest
– General Configuration	General PLC Runtime Configuration	user
– WebVisu	PLC WebVisu	guest
Networking		
– Host/Domain Name	Configuration of Host and Domain Name	user
– TCP/IP	TCP/IP Configuration	user
– Ethernet	Ethernet Configuration	user
– Routing	Routing	user
Firewall		
– General Configuration	General Firewall Configuration	user
– MAC Address Filter	Configuration of MAC Address Filter	user
– User Filter	Configuration of User Filter	user
Clock	Configuration of Time and Date	user
Administration		
– Users	Configuration of the users for the Web-based Management	admin
– Create Image	Create bootable Image	admin
– Serial Interface	Configuration of Serial Interface RS233	admin

Table 43: Access Rights for WBM Pages

Navigation	WBM page	User
– Service Interface	Configuration of Service Interface	admin
– Reboot	Reboot Controller	admin
Package Server		
– Firmware Backup	Firmware Backup	admin
– Firmware Restore	Firmware Restore	admin
– System Partition	System Partition	admin
Mass Storage	Mass Storage	admin
Software Uploads	Software Uploads	admin
Ports and Services		
– Network Services	Configuration of Network Services	user
– NTP Client	Configuration of NTP Client	user
– PLC Runtime Services	Configuration of PLC Runtime Services	user
– SSH	SSH Server Settings	user
– TFTP	TFTP Server	user
– DHCP	DHCP Configuration	user
– DNS	Configuration of DNS Service	user
– Modbus	Modbus Services Configuration	user
Cloud Connectivity	Configuration of Cloud Connectivity	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
Diagnostic	Diagnostic Information	guest
BACnet		
– General	Configuration of General BACnet	admin
– Storage Location	Configuration of BACnet Storage Location parameters	admin
– Diagnostic	BACnet Diagnostic Information	admin
OpenVPN / IPsec	Configuration of OpenVPN / IPsec	admin
Security		
– TLS	Security Settings	admin
– Integrity	Advanced Intrusion Detection Environment (AIDE)	admin
Legal Information		
– Open Source Licenses	Open Source Licenses	guest
– WAGO Licenses	WAGO Licenses	guest

7.8.1.2 General Information about the Page

The screenshot displays the WAGO Web-based Management (WBM) interface. At the top, the WAGO logo is followed by the text 'Web-based Management' and 'WAGO 750-8206 PFC200 CS 2ETH RS CAN DPS'. A 'Login' link is visible on the right. The main content area is divided into three sections:

- Navigation:** A tree view on the left with categories like Information, PLC Runtime, Networking, Firewall, Clock, Administration, Package Server, Mass Storage, Software Uploads, Ports and Services, Cloud Connectivity, SNMP, Diagnostic, PROFIBUS DP, OpenVPN / IPsec, Security, and Legal Information.
- Status Information:** A central panel showing controller and network details.
 - Controller Details:**
 - Product Description: WAGO 750-8206 PFC200 CS 2ETH RS CAN DPS
 - Order Number: 750-8206
 - License Information: Codesys-Runtime-License
 - Firmware Revision: 02.08.25(11)
 - Network Details X1/X2:**
 - State: ☒ enabled
 - MAC Address: 00:30:de:40:0e:6f
 - IP Address: 192.168.1.17 (static)
 - Subnet Mask: 255.255.255.0
- Status:** A panel on the right showing system status.
 - WBM:** ☐
 - Local Time:** 10:16
 - Local Date:** 09.04.2018
 - PLC Switch:** RUN
 - LEDs:** A grid of status indicators for BF, DIA, U4, U3, U2, U1, SYS, RUN, IO, MS, NS, and CAN.

At the bottom, a footer line reads: 'WAGO • Hansastr. 27 • D-32423 Minden • WAGO is a registered trademark of WAGO Verwaltungsgesellschaft mbH.'

Figure 32: WBM Browser Window (Example)

The device name is displayed in the header of the browser window. When the user has logged out, a **[Login]** button is displayed on the right in the header line, when logged in a **[Logout]** button is displayed.

The navigation tree is shown on the left of the browser window. You can use this navigation tree to go to the individual pages and, where provided, subpages included in these pages. Some pages can only be called after a successful login. To log in click the **[Login]** button and enter the user name and password in the login window.

A status area with the following elements is displayed on the right:

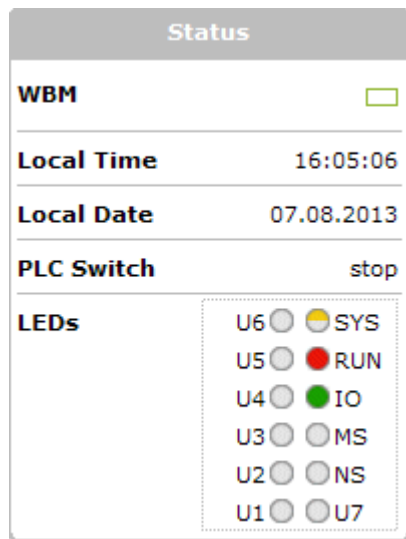


Figure 33: WBM Status Information (Example)

- **WBM status:**
This indicates whether the WBM is currently communicating with the device in the background. In other words, one or more requests have been sent and the browser is waiting for a response. Movement is then visible in the graphic. This occurs when data is read on initial call-up of the page, when the user has sent off a change form or when data is reloaded automatically in cycles, e.g., the contents of the status area.
- **Local Time:**
Local time on the device
- **Local Date:**
Local date on the device
- **PLC Switch:**
Setting of the mode selector switch
- **LEDs:**
This indicates the status of the device LEDs. 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.

7.8.1.3 “Status Information” Page

The following tables explain the parameters listed on this page:

7.8.1.3.1 “Controller Details” Group

This group displays the properties of the controller.

Table 44: WBM “Status Information” Page – “Controller Details” Group

Parameter	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

7.8.1.3.2 “Network Details Xn” Group(s)

This group displays the network and interface properties of the controller.

If the switch is enabled, one group (“Network Details X1/X2”) is shown for both connections.

If the switch is disabled, a separate group (“Network Details X1” / “Network Details X2”) is shown for each connection.

Table 45: WBM "Status Information Page – "Network Details Xn" Group(s)

Parameter	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

7.8.1.4 “PLC Runtime Information” Page

Information about the enabled runtime system and PLC program created in the programming software is provided on the “PLC Runtime Information” page.

7.8.1.4.1 “PLC Runtime” Group

Table 46: WBM “PLC Runtime Information” Page – “PLC Runtime” Group

Parameter	Explanation
Version	The version of the currently enabled runtime system is shown. If the runtime system is disabled, “None” is displayed.

7.8.1.5 “General PLC Runtime Configuration” Page

The settings for the boot project created with the programming software are given on the “General PLC Runtime Configuration” page.

7.8.1.5.1 “General PLC Runtime Configuration” Group

Table 47: WBM “General PLC Runtime Configuration” Page – “General PLC Runtime Configuration” Group

Parameters	Explanation	
PLC runtime version	Select here the PLC runtime system to be enabled.	
	None	No runtime system is enabled.
	<i>e!RUNTIME</i>	<i>e!RUNTIME</i> runtime system is enabled.
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



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.

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

The runtime system change is effective immediately.

The home directory change takes effect after the next restart.

7.8.1.6 “PLC WebVisu” Page

The settings for the web visualization created in the runtime system are shown on the “PLC WebVisu” page.

7.8.1.6.1 “Webserver Configuration” Group

Table 48: WBM “PLC WebVisu” Page – “Webserver Configuration” Group

Display Fields	Explanation	
e!RUNTIME Webserver State	This indicates the status (enabled/disabled) of the <i>e!RUNTIME</i> Webserver.	
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.
	Web-Visu	The web visualization of the runtime system is displayed.

Click **[Submit]** to apply change. The change is effective 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 Web server 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 controller using web visualization.

7.8.1.7 “Configuration of Host and Domain Name” Page

The settings for the general TCP/IP parameters are found on the “Configuration of Host and Domain Name” page.

7.8.1.7.1 “HostName” Group

Table 49: WBM “Configuration of Host and Domain Name” Page – “Hostname” Group

Parameters	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 here the hostname of your 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 **[Submit]** to apply the change. The change is effective immediately.



Note

CODESYS OPC-UA server does not accept host names until after a restart!

If you are using the CODESYS OPC-UA server, you must restart the controller after any changes are made in order for the changes to be applied by CODESYS OPC-UA server.

If a hostname is supplied via a DHCP response, this is enabled in the system. If there are several network interfaces with DHCP always the last received hostname is valid.

If only the hostname configured here is to be valid, the configuration of the DHCP server must be adapted so that no hostnames are transferred in the DHCP response.

7.8.1.7.2 “Domain Name” Group

Table 50: WBM “Configuration of Host and Domain Name” Page – “Domain Name” Group

Parameters	Explanation
Currently used	The domain name currently used is displayed. It may differ from the configured domain name if you have selected dynamic assignment of an IP address via DHCP or BootP.
Configured	Enter the domain name. The default entry is “localdomain.lan”.

Click **[Submit]** to apply the change. The change is effective immediately.

If a domain name is supplied via a DHCP response, this is enabled in the system.
If there are several network interfaces with DHCP, the last received domain name is always valid.

If only the domain name configured here is to be valid, the configuration of the DHCP server must be adapted so that no domain names are transferred in the DHCP response.

7.8.1.8 “TCP/IP Configuration” Page

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

7.8.1.8.1 “IP Configuration (Xn)” Group(s)

If the switch is enabled, one group (“IP Configuration”) is shown for both connections.

If the switch is disabled, a separate group (“IP Configuration X1” / “IP Configuration X2”) is shown for each connection.

Table 51: WBM “TCP/IP Configuration” Page – “IP Configuration (Xn)” Group(s)

Parameters	Explanation	
Configuration Type	Select a static or dynamic IP address.	
	Static IP	Static IP addressing
	DHCP	Dynamic IP addressing
	BootP	Dynamic IP addressing
IP Address	Enter here a static IP address. This is enabled if “Static IP” is enabled in the Configuration Type field.	
Subnet Mask	Enter the subnet mask. This is enabled if “Static IP” is enabled in the Configuration Type field.	

Click **[Submit]** to apply changes. The changes are effective immediately.

7.8.1.8.2 “Default Gateway n” Groups

You can configure two default gateways. The controller transmits all network data not going to a station on the local network to a default gateway. First the gateway with the lowest metric is addressed. If this is not reached, the second gateway is used. The selection is random if the metric is the same.

A default gateway can also be configured via DHCP. These default gateways are given the metric 10, by which they are normally used before the static gateways.

Table 52: WBM “TCP/IP Configuration” Page – “Default Gateway n” Group

Parameters	Explanation	
Gateway enabled	Set here whether the selected default gateway is to be used.	
	Disabled	The default gateway is not used.
	Enabled	The default gateway is used.
Destination Address	Enter here if any network devices or only a specific network device or device pool is to be accessed.	
	“default”	Any network devices can be reached.
	Network address	Only a specific network device or device from the set address pool can be reached.
Destination Mask	Enter the subnet mask of the station. If “default” is entered at Destination Address , the value “0.0.0.0” must be entered here.	
Gateway Address	Enter the address of the default gateway.	
Gateway Metric	Set here a number as the metric. With multiple default gateways, the metric defines the gateway to which data packets are first sent. Priority is given to the gateway with the lower metric. The default value for the metric is 20. The lowest value is 0. The highest value is 4.294.967.295.	

Click **[Submit]** to apply the change. The change is effective immediately.

7.8.1.8.3 “DNS Server” Group

Table 53: WBM “TCP/IP Configuration” Page – “DNS Server” Group

Parameters	Explanation
Configured: None/ DNS Server n	The addresses of the defined DNS servers are displayed. If no server has been defined, “Configured: None” is displayed.
New Server IP	Add additional DNS addresses. You can enter 10 addresses.
Additionally used (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), “none” is displayed.

Click **[Delete]** to remove the selected DNS server. The change is effective immediately.

Click **[Add]** to add the entered DNS server. The change is effective immediately.

7.8.1.9 “Ethernet Configuration” Page

The settings for Ethernet TCP/IP are located on the “Ethernet Configuration” page.

7.8.1.9.1 “Switch Configuration” Group

Table 54: WBM “Ethernet Configuration” Page – “Switch Configuration” Group

Parameter	Explanation	
Interfaces	Enable or disable the switch.	
	Switched	Both interfaces are operated with one IP address.
	Separated	Each interface is operated with its own IP address.
Port Mirror	Enable or disable the mirroring of the data traffic between the ports.	
	None	Both Ethernet ports 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.
Fast Aging enabled	Set here the aging time of unused entries in the list of MAC addresses with a port assignment to external network stations. This field is only enabled in “switched” mode. Fast aging is only effective in this mode.	
	Disabled	An unused address entry becomes obsolete after 200 seconds.
	Enabled	An unused address entry becomes obsolete after 800 microseconds.
Broadcast Protection	Set here the broadcast limit for protection against overloads.	
	Disabled	No limitation of broadcast packets.
	1 % ... 5 %	Limitation of incoming broadcast packets to the selected percentage of the total possible data throughput (10/100Mbit).
Rate Limit	Set here the basic limitation of the incoming data traffic.	
	Disabled	No limitation of the incoming data traffic
	64 kbps ... 99 mbps	Limitation of the incoming data traffic to the entered value

Click **[Submit]** to apply the change. The change is effective immediately.

7.8.1.9.2 “Interface Xn” Groups

One group (“Interface X1” / “Interface X2”) is displayed for each connection.

Table 55: WBM “Ethernet Configuration” Page – “Interface Xn” Groups

Parameter	Explanation	
Enabled	You can enable or disable the interface.	
Autonegotiation on	When Autonegotiation is enabled, the connection modalities are negotiated automatically with the peer devices.	
Speed/Duplex	Select the transmission speed and the duplex method:	
	10 Mbit half-duplex	Information can only be sent or received.
	100 Mbit half-duplex	
	10 Mbit full-duplex	Information can be sent and received simultaneously.
	100 Mbit full-duplex	

Click **[Submit]** to apply changes. The changes are effective immediately.

7.8.1.10 “Routing” Page

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

7.8.1.10.1 “General Routing Configuration” Group

Table 56: WBM “Routing” Page – “General Routing Configuration” Group

Parameter	Explanation
Routing enabled entirely	Specify here 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 PFC on one network interface to leave the PFC 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.

7.8.1.10.2 “Static Routes” Group

Each configured static route has its own area in the display.

To maintain compatibility with earlier firmware versions, at least two routing entries always exist. These can be disabled, but not removed. If a route is either removed or disabled, it is no longer entered in the system.

Table 57: WBM “Routing” Page – “Static Routes” Group

Parameter	Explanation	
Enabled	Specify here whether the selected route should be used.	
	Disabled	The route is not used.
	Enabled	The route is used.
Destination Address	Specify here 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 here. If “default” is entered for Destination Address, the value “0.0.0.0” must be entered here.	
Gateway Address	Enter the address of the gateway here.	
Gateway Metric	Set the number used as the metric here. 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 default value for the metric is 20. The lowest value is 0. The highest value is $2^{32}-1 = 4,294,967,295$.	

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.

7.8.1.10.3 “Dynamic Routes” Group

All default gateways received via DHCP are displayed here.
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.

7.8.1.10.4 “IP Masquerading” Group

Each entry has its own area in the display.

Table 58: WBM “Routing” Page – “IP-Masquerading” Group

Parameter	Explanation	
Enabled	Specify here whether IP masquerading should be used for the selected network interface.	
	Disabled	IP masquerading is not used.
	Enabled	IP masquerading is used.
Interface	You can select the specified name of a network interface here. 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 “Routing enabled entirely” 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.

7.8.1.10.5 “Port Forwarding” Group

Each entry has its own area in the display.

Table 59: WBM “Routing” Page – “Port Forwarding” Group

Parameter	Explanation	
Enabled	Specify here 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 here. Alternatively, selecting “other” allows you to specify any network interface name.	
Port	Enter the port here on which the controller receives network data packets that are to be forwarded.	
Protocol	Here 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 here. This address replaces the original destination address of the network data packet.	
Destination Port	Specify the port number of the destination device here. 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 “Routing enabled entirely” 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.

7.8.1.11 “General Firewall Configuration” Page

7.8.1.11.1 “Global Firewall Parameters” Group

Table 60: WBM “General Firewall Configuration” Page – “Global Firewall Parameters” Group

Parameters	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.
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 is effective immediately.

7.8.1.11.2 “Firewall Parameters Interface xxx” Group

These settings in this group refer to the configuration of the firewall at IP level.

Table 61: WBM “General Firewall Configuration” Page – “Firewall Parameter Interface xxx” Group

Parameters	Explanation	
Firewall enabled for Interface	Enable or disable the firewall for the specific interface.	
ICMP echo protection	Enable or disable the “ICMP echo” protection for the respective interface.	
ICMP echo limit per second	You can specify the maximum number of “ICMP echo bursts” per second. “0” = “Disabled”	
ICMP burst limit	You can specify the maximum number of “ICMP echo bursts” per second. “0” = “Disabled”	
Service enabled	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.
	FTP	
	FTPS	
	HTTP	
	HTTPS	
	I/O-CHECK	
	PLC Runtime	
	PLC WebVisu – direct link (port 8080)	
	SSH	
	TFTP	
	BootP/DHCP	
	DNS	
	Modbus TCP	
	Modbus UDP	
	SNMP	
	OPC UA	

Click **[Submit]** to apply the change. The change is effective immediately.

7.8.1.12 “Configuration of MAC Address Filter” Page

You set the firewall configuration at ETHERNET level on this page.

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 activated 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!

7.8.1.12.1 “Global MAC Address Filter State” Group

Table 62: 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 here.

Click **[Submit]** to apply change. The change is effective immediately.

7.8.1.12.2 “MAC Address Filter State Xn” Group

Table 63: WBM “Configuration of MAC Address Filter” Page – “MAC Address Filter State Xn” Group

Parameters	Explanation
Filter enabled	Enable or disable here the MAC address filter for the specific interface.

Click **[Submit]** to apply change. The change is effective immediately.

7.8.1.12.3 “MAC Address Filter Whitelist” Group

Table 64: 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 here.
...	
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 here.
Filter enabled	Enable or disable the filter for the new list entry here.

Click **[Submit]** to apply the change. The change is effective immediately.

Click the appropriate **[Delete]** button to remove an existing list entry. The change is effective immediately.

Click **[Add]** to accept a new list entry. You can enter 10 filters. The change is effective immediately.

7.8.1.13 “Configuration of User Filter” Page

7.8.1.13.1 “User Filter” Group

Table 65: WBM “Configuration of User Filter” Page – “User Filter” Group

Parameters	Explanation
Count	The number of configured user filters is displayed.

7.8.1.13.2 “User Filter n” Group

Table 66: WBM “Configuration of User Filter” Page – “User Filter n” Group

Parameters	Explanation
Source IP address	The source IP address for the respective filter entry is displayed.
Source netmask	This displays the source network for the corresponding filter entry.
Source port	The source port number for the respective filter entry is displayed.
Destination IP address	The destination IP address for the respective filter entry is displayed.
Destination subnet mask	The destination network mask for the respective filter entry is displayed.
Destination port	The designation port number for the respective filter entry is displayed.
Protocol	The permitted protocols for the respective filter is displayed.
Input interface	The permitted interfaces for the respective filter are displayed.
Policy	This displays whether the network device is allowed or excluded by the filter.

Click the appropriate **[Delete]** button to remove a configured filter. The change is effective immediately.

7.8.1.13.3 “Add New User Filter” Group

You can enter 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.

Table 67: WBM “Configuration of User Filter” Page – “Add New User Filter” Group

Parameters	Explanation	
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 entry.	
Source netmask	Enter here the source network mask for the new filter entry.	
Source port	Enter here the source port address for the new filter entry.	
Destination IP address	Enter here the destination IP address for the new filter entry.	
Destination subnet mask	Enter here the destination network mask for the new filter entry.	
Destination port	Enter the destination port number for the new filter entry.	
Protocol	Enter here the permitted protocols for the new filter.	
	TCP	The TCP service is permitted.
	UDP	The UDP service is permitted.
Input interface	Enter here the permitted interfaces for the new filter.	
	X1	The X1 interface is permitted.
	X2	The X2 interface is permitted.
	VPN	The VPN interface is permitted.

To accept the new filter click **[Add]**. The change is effective immediately.

7.8.1.14 “Configuration of Time and Date” Page

The settings for date and time are shown on the “Configuration of Time and Date” page.

7.8.1.14.1 “Date on Device” Group

Table 68: WBM “Configuration of Time and Date” Page – “Date on Device” Group

Parameters	Explanation
Local	Set date.

Click **[Change date]** to apply change. The change is effective immediately.

7.8.1.14.2 “Time on Device” Group

Table 69: WBM “Configuration of Time and Date” Page – “Time on Device” Group

Parameters	Explanation
Local	Set local time.
UTC	Set GMT time.
12 h format	For switching between 12-hour and 24-hour time display

Click **[Change time]** to apply change to the time. The change is effective immediately.

Click **[Change format]** to apply change to the time format. The change is effective immediately.

7.8.1.14.3 “Time Zone” Group

You can specify the appropriate time zone for your location in this group.

The total number of possible time zones is over 500. A complete listing would exceed the scope of this documentation.

Due to the large number of time zones, the selection is limited via the “Time Zone” parameter.

You can select further time zones with the “TZ String” parameter.

Table 70: WBM “Configuration of Time and Date” Page – “Time Zone” Group

Parameters	Explanation	
Time zone	Specify the appropriate time zone for your location.	
	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”

* Default setting

Click **[Change]** to apply time zone change. The change is effective immediately.

7.8.1.14.4 “TZ String” Group

In this group you can enter a time zone that is not contained in the “Time Zone” selection.

If the controller can associate the TZ string entered with a known time zone that had been missing from the “Time Zone” selection, this time zone is then also added to the “Time Zone” list.

You can find information on time zones and the corresponding “TZ strings” on the Internet.

For example, to indicate the pure UTC time, enter the TZ string “UTC0.”

If no unique association is possible, the text “Unknown” is displayed for the “Time Zone” selection.

Table 71: WBM “Configuration of Time and Date” Page – “TZ String” Group

Parameters	Explanation
TZ string	You can enter the name of the time zone or the country and city here.

Click **[Change]** to apply the change. The change is effective immediately.

7.8.1.15 “Configuration of the Users for the Web-based Management” Page

The settings for user administration are shown on this page.

7.8.1.15.1 “Change Password for Selected User” Group



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.

Table 72: WBM “Configuration of the users for the Web-based Management” Page – “Change Password for Selected User” Group

Parameters	Explanation
Select User	Select the user (“user” or “admin”) for new password assignment.
New Password	Enter the new password for the user selected under “Select User”. The following ASCII characters for passwords are valid: a ... z, A ... Z, 0 ... 9 and spaces. These special characters are also valid:]!"#\$%&'()*+,-./:;<=>?@[^_`{ }~-
Confirm Password	Enter the new password again for confirmation.
Old Password	Enter the currently used password for authentication.

Click **[Change Password]** to apply change. The change is effective immediately.



Note

Observe the valid characters for WBM passwords!

If WBM passwords with invalid characters are set outside the WBM system (e.g. via CBM), then accessing the WBM pages is no longer possible!



Note

Observe access rights

Authorized WBM users only have access to the Web pages. User administration for controller applications is configured separately.

7.8.1.16 “Create Bootable Image” Page

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

7.8.1.16.1 "Create Bootable Image from Active Partition (<Active Partition>" Group

The active partition that boot-up was performed from is displayed in brackets in the heading.

Table 73: WBM “Create Bootable Image” page – “Create bootable image from active partition” Group

Parameters	Explanation		
Destination	The possible destination partition that an image will be saved to is displayed. 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
Size of created image	Define the size of the image on the memory card. This field is only visible when “Memory Card” is set as the target.		
	Reduced to content	The storage space of the copied image is kept as small as possible.	
	Full card size	The image is created so that the entire memory card is filled.	

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

- 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 definitively 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.



Note

Remove the memory card write protection!

Because write access to the memory card is possible during the boot process, the memory card cannot be write protected when creating the image and during operation.

7.8.1.17 “Configuration of Serial Interface RS232” Page

The settings for the serial interface are shown on the “Configuration of Serial Interface RS232” page.

7.8.1.17.1 “Serial Interface Assigned to” Group

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

7.8.1.17.2 “Assign Owner of Serial Interface (Active after Next Controller Reboot)” Group

You can specify the application that the serial interface is assigned to after the next controller reboot.

Table 74: WBM “Configuration of Serial Interface RS232” Page – “Assign Owner of Serial Interface” Group

Parameters	Explanation
Linux® Console	Specify that the serial interface is assigned to the Linux® console.
Unassigned (usage by applications, libraries, CODESYS)	Specify that the serial interface is not to be assigned to any particular application and is available, so that the CODESYS program, for example, can access it via function blocks.

NOTICE

Remove RS-485 devices before switching to “Linux Console”!

Connected RS-485 devices can be damaged when switching to “Linux Console”.
Remove these devices before switching!

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

7.8.1.18 “Configuration of Service Interface” Page

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

7.8.1.18.1 “Service Interface assigned to” Group

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

7.8.1.18.2 “Assign Owner of Service Interface (enabled after next controller reboot)” Group

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

Table 75: WBM “Configuration of Serial Interface RS-232” 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 **[Change Owner]** to apply the change. 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!

7.8.1.19 “Reboot Controller” Page

The settings for the system reboot are shown on the “Reboot Controller” page.

7.8.1.19.1 “Reboot Controller” Group

Click the **[Reboot]** button to reboot the system.



Note

Account for boot-up time!

The boot process takes time. You cannot access the controller while this is occurring.

7.8.1.20 “Firmware Backup” Page

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

Table 76: “Firmware-Backup” WBM Page

Parameters	Explanation	
Packages	You can select the data to be backed up here. To do this, select the corresponding entries.	
	All	All data is backed up. This selection is only enabled if the memory card is selected as the target.
	PLC runtime project	The PLC runtime project is backed up.
	Settings	The controller settings are backed up.
	System	The controller operating system is backed up.
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 without system data is inserted.
	Network	The data are stored on the file system and can then be downloaded to the PC.
Activate “auto update feature”	To start the automatic update when a memory card with system data is inserted, select this button.	

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.

To begin the backup procedure, click the **[Submit]** button.

7.8.1.21 “Firmware Restore” Page

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

Table 77: “Firmware Restore” WBM Page

Parameters	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 without system data is inserted.
	Network	The data is uploaded from the PC and restored.
Packages	Select the data to be restored here. To do this, select the corresponding entries.	
	All	All data is restored. This selection only appears if the memory card is selected as the data source.
	PLC runtime project	The PLC runtime project is restored.
	Settings	The controller settings are restored.
	System	The controller operating system is loaded. The current controller settings are retained.
CODESYS backup file	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 backup file	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 backup file	Enter the name of the backup file for the system data here. The input field only appears if the network is selected as the data source.	

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



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.

Click the **[Browse]** button to select the files in Explorer. The buttons only appear if the network is selected as the data source.

To start the restore procedure, click the **[Submit]** button.

7.8.1.22 “System Partition” Page

The settings for specifying the partition that the system will be started from are shown on the “System Partition” page.

7.8.1.22.1 “Current Active Partition” Group

The partition currently in use is displayed here.

7.8.1.22.2 “Set Inactive Partition Active” Group

Click **[Activate Partition]** to start the system from a different partition at the next controller reboot.



Note

Ensure bootable partition!

A functional firmware backup must be present in the boot partition!

7.8.1.23 “Mass Storage” Page

A group containing information about the storage volume is displayed for each storage volume that is found, along with an additional group for formatting (when this is possible).

The group title contains the designation for the storage volume (“SD card” or “Internal Flash”) and, if this storage volume is also the active partition, the text “Active Partition”.

7.8.1.23.1 “<Device Name>” Group(s)

Table 78: WBM “Mass Storage” Page – “<Device Name>” Group

Parameters	Explanation
Device	The name of the storage volume in the operating system file system is displayed here.
Volume name	The name of the storage volume is displayed here.

7.8.1.23.2 “<Device Name> - create new filesystem” Group(s)

Table 79: WBM “Mass Storage” Page – “<Device Name> - create new filesystem” Group

Parameters	Explanation
Filesystem type	Here you can select the format in which the file system should be created on the memory card.
	Ext4 The file system is created in Ext4 format. The files are not readable under Windows!
	FAT The file system is created in FAT format.
Volume Name	Specify the name for the storage volume when formatted.

Note



Data are deleted!

Any data stored in the storage volume is deleted during formatting!

To format the specified storage volume, click **[Start Formatting]**.

Note



FAT formatting for BACnet data!

Format the memory card as FAT to save recorded trend log, event log, or persistent BACnet data to the memory card.

7.8.1.24 “Software Uploads” Page

The settings for a device update are shown on the “Software Uploads” page.

7.8.1.24.1 “Upload New Software” Group

Table 80: WBM “Software Uploads” Page – “Upload New Software” Group

Parameter	Explanation
Software Files	You can select fieldbus software, program licenses and update scripts, for example, for transfer from a PC to the controller.

To select a file on the PC, click the **[Browse]** button.

To transfer the selected file to the controller, click **[Start Upload]** button.

7.8.1.24.2 “Activate New Software” Group

Table 81: WBM “Software Uploads” Page – “Activate New Software” Group

Parameter	Explanation
Software File	This shows the file name of the transferred software package. If no new uploaded software package is present on the controller, the message “No upload file exists” is displayed.
Action	Select here the action required.
	Activate The transferred software package is activated.
	Force (Manual reboot afterward s needed) Installs a transferred software package that cannot be activated with “Activate.” Required for activating a controller reboot. The software package is activated on reboot.
	Discard (delete upload) The transferred software package is deleted again by the controller.

To perform the action, click the **[Submit]** button. The process starts immediately.

The file with the software package is deleted again after the installation is completed or when the controller is restarted.

7.8.1.25 “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, enhance your cyber security, close all ports and services in the control components (e.g., 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.

Besides enabling/disabling the individual services, you can also limit the services for each particular interface via the firewall on the “General Firewall Configuration” page.

7.8.1.25.1 “Telnet” Group

Table 82: WBM “Configuration of Network Services” Page – “Telnet” Group

Parameter	Explanation
Service active	Enable/disable the Telnet service here.

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

7.8.1.25.2 “FTP” Group

Table 83: WBM “Configuration of Network Services” Page – “FTP” Group

Parameter	Explanation
Service active	Enable/disable the FTP service here.

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

7.8.1.25.3 “FTPS” Group

Table 84: WBM “Configuration of Network Services” Page – “FTPS” Group

Parameter	Explanation
Service active	Enable/disable the FTPS service here.

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

7.8.1.25.4 “HTTP” Group

Table 85: WBM “Configuration of Network Services” Page – “HTTP” Group

Parameter	Explanation
Service active	Enable/disable the HTTP service here.

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



Note

Disconnection abort on disabling

If the HTTP service is disabled, the connection to the controller may be interrupted. Then open the WBM page again.

7.8.1.25.5 “HTTPS” Group

Table 86: WBM “Configuration of Network Services” Page – “HTTPS” Group

Parameter	Explanation
Service active	Enable/disable the HTTPS service here.

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



Note

Disconnection abort on disabling

If the HTTPS service is disabled, the connection to the controller may be interrupted. Then open the WBM page again.

7.8.1.25.6 “WAGO-I/O-CHECK” Group

Table 87: WBM “Configuration of Network Services” Page – “I/O-CHECK” Group

Parameter	Explanation
Service active	Enable/disable the WAGO-I/O-CHECK service here.

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

7.8.1.25.7 “OPC UA” Group

Table 88: WBM “Configuration of Network Services” Page – “OPC UA” Group

Parameter	Explanation
Service active	Enable/disable the OPC UA service here.

Click the **[Submit]** button to apply the changes. 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!

7.8.1.26 “Configuration of NTP Client” Page

The settings for the NTP service are shown on the “Configuration of NTP Client” page.

7.8.1.26.1 “NTP Client Configuration” Group

Table 89: WBM “Configuration of NTP Client” Page – “NTP Client Configuration” Group

Parameters	Explanation	
Service enabled	Enable/disabled time update.	
Service Result	This displays whether time data was accessible and updated via NTP. This field is only displayed with the NTP service enabled.	
	Time server not available until now	The time data was not yet updated.
	Time server available	The time data was updated.
Time Server n	Enter here the IP addresses of up to 4 time servers. Time server No. 1 is requested first of all. If no data is accessible via this server, time server No. 2 is requested etc.	
Update interval (sec)	Specify here the update interval of the time server.	
Additionally used (assigned by DHCP)	The NTP servers assigned if necessary by DHCP (or BootP) are displayed. If no NTP server has been assigned by DHCP (or BootP), “none” is displayed.	

Click the **[Submit]** button to apply the changes. The changes are effective immediately.

7.8.1.26.2 “NTP Single Request” Group

To update the time immediately, irrespective of the update interval, click **[Update Time Now]**.

7.8.1.27 “Configuration of PLC Runtime Services” Page

The settings for various services of the enabled runtime system are shown on the “Configuration of PLC Runtime Services” page.

7.8.1.27.1 “General Configuration” Group

Table 90: WBM “Configuration of PLC Runtime Services” Page – “General Configuration” Group

Parameters	Explanation
Port Authentication Password	Enter the new password for port authentication.
Confirm Password	Enter the new password again for confirmation.

Click **[Submit]** to apply change. The change is effective immediately.

7.8.1.27.2 “e!RUNTIME” Group

Table 91: WBM “Configuration of CODESYS Services” Page – “e!RUNTIME Webserver” Group

Parameters	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 is specified under “General Configuration”.

Click **[Submit]** to apply change. The change is effective immediately.

7.8.1.28 “SSH Server Settings” Page

The settings for the SSH service are shown on the “SSH Server Settings” page.

7.8.1.28.1 “SSH Server” Group

Table 92: WBM “SSH Server Settings” Page – “SSH Server” Group

Parameter	Explanation
Service active	You can enable/disable the SSH server here.
Port Number	Specify the port number here.
Allow root login	You can enable or inhibit root access.
Allow password login	Activate or deactivate the password query function here.

Click on **[Submit]** to accept the changes. The changes will be effective immediately.

7.8.1.29 “TFTP Server” Page

The settings for the TFTP service are shown on the “TFTP Server” page.

7.8.1.29.1 “TFTP Server” Group

Table 93: WBM “TFTP Server” Page – “TFTP Server” Group

Parameter	Explanation
Service active	Activate or deactivate the TFTP server.
Download directory	Specify here the path for downloading the server directory.

Click on **[Submit]** to accept the changes. The changes will be effective immediately.

7.8.1.30 “DHCP Configuration” Page

The settings for the DHCP service are shown on the “DHCP Configuration” page.

7.8.1.30.1 “DHCP Configuration Xn” Group

Table 94: WBM “DHCP Configuration” – “DHCP Configuration Xn” Group

Parameter	Explanation
Service active	Enable or disable the DHCP service for the interface Xn.
IP Range	Enter here a range of available IP addresses.
Lease time (sec)	Specify the lease time here in seconds. 120 seconds are entered by default.
Static hosts/ Static host n	This displays the static assignments of MAC IDs to IP addresses. If no assignment was defined, “No static hosts configured” is displayed.
New static host	Enter here 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 10 assignments.

Click on **[Submit]** to accept the changes. The changes will be effective immediately.

Click on **[Add]** to accept a new assignment. The change is effective immediately.

Click on **[Delete]** to delete an existing assignment. The change is effective immediately.

7.8.1.31 “Configuration of DNS Service” Page

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

7.8.1.31.1 “DNS Service” Group

Table 95: WBM “Configuration of DNS Service” Page – “DNS Service” Group

Parameter	Explanation	
Service active	You can enable/disable the DNS server service here.	
Mode	Select here 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 static assignments of IP addresses to names. If no assignment was defined, “No static hosts configured” is displayed.	
New static host	Enter here a new static assignment, e.g., “192.168.1.20:hostname.” You can enter 10 assignments.	

Click on **[Submit]** to accept the changes. The changes will be effective immediately.

Click on **[Add]** to accept a new assignment. The change is effective immediately.

Click on **[Delete]** to delete an existing assignment. The change is effective immediately.

7.8.1.32 “Modbus Services Configuration” Page

The settings for various Modbus services are shown on the “Modbus Services Configuration” page. The groups are only visible if the **e!RUNTIME** system is enabled. Otherwise an information text is displayed.

7.8.1.32.1 “Modbus TCP” Group

Table 96: WBM “Modbus Services Configuration” Page – “Modbus TCP” Group

Parameter	Explanation
Service active	Disable or enable the Modbus/TCP service here.

Click the **[Submit]** button to apply the changes. The change is effective immediately.

7.8.1.32.2 “Modbus UDP” Group

Table 97: WBM “Modbus Configuration Services” Page – “Modbus UDP” Group

Parameter	Explanation
Service active	Disable/enable the Modbus-UDP service here.

Click the **[Submit]** button to apply the changes. The change is effective immediately.

7.8.1.33 “Configuration of Cloud Connectivity” Page

On the page “Configuration of Cloud Connectivity” you can find the settings and information for cloud access.



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 at www.wago.com!

7.8.1.33.1 “Software Version” Group

Table 98: WBM “Configuration of Cloud Connectivity” Page – “Software Version” Group

Parameter	Explanation
Version	The cloud plug-in version is displayed.

7.8.1.33.2 “Status” Group

Table 99: WBM “Configuration of Cloud Connectivity” Page – “Status” Group

Parameter	Explanation
Operation	The status of the cloud connectivity application is displayed here.
Data collections	This shows how many data collections have been registered on the IEC application side for transfer to the cloud.
Connection	The status of the connection to the cloud service is shown here.
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.

7.8.1.33.3 “Settings” Group

The parameters indicated depend on the cloud platform setting and, if applicable, on other settings in this group.

Table 100: WBM “Configuration of Cloud Connectivity” Page – “Settings” Group

Parameter	Explanation
Service enabled	You can enable/disable the cloud connectivity function here.
Cloud platform	Select the cloud platform here.
Hostname	Enter the host name or IP address for the selected cloud platform here.
Group ID	Here you can specify the group in which the edge node ID should be placed.
Device ID	Enter the device ID for the selected cloud platform here.
Client ID	Enter the client ID for the selected cloud platform here.
Edge Node ID	Enter the edge node ID for the selected cloud platform here.
Activation Key	Enter the activation key for the selected cloud platform here.
Clean Session	Here you can 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	Here you can specify whether TLS encryption should be used for the connection to the cloud platform. Amazon Web Services (AWS) always uses TLS.
Port	Enter the port here to which a connection is to be established. Typical values are 8883 for encrypted connections and 1883 for unencrypted connections.
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 <code>/etc/ssl/certs/ca-certificates.crt</code> , which is already installed on the PFC.
User	Enter the user name for cloud service authentication here.
Password	Enter the password for cloud service authentication here.
Certification file	Enter the path here to the file encoded in PEM format that is used for cloud service authentication.

Table 100: WBM "Configuration of Cloud Connectivity" Page – "Settings" Group

Parameter	Explanation
Key file	Enter the path here 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 box is not checked, the connection to the cloud platform will be set up using the MQTT protocol via Port 8883.
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 here 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. (You can find more information in Application Note A500920.)
Last Will	Here you can specify whether a last will message should be enabled/disabled.
(Last Will) Topic	Here you can specify the topic under which the last will messages should be sent.
(Last Will) Message	Here you can enter the message you wish to use as the last will message.
(Last Will) QoS	Here 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 here whether a device info message should be generated that informs the cloud service of the basic configuration of the PFC. (You can find more information in Application Note A500920.)
Device status	Specify here whether device state messages should be generated that inform the cloud service about changes in the mode selector switch and the LEDs. (You can find more information in Application Note A500920.)
Standard commands	Specify here whether the integrated standard commands should be supported. (You can find the list of standard commands in Application Note A500920.) If the check box is disabled, only the commands defined in the IEC program are supported.

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 table shows the dependencies of the selection and input fields for the selected cloud platform.

Table 101: Dependencies of the Selection and Input Fields for the Selected Cloud Platform

Selection or Input Field	Cloud Platform							Data Protocol				Last Will
	WAGO Cloud	Azure	MQTT AnyCloud	IBM Cloud	Amazon Web Services	SAP IoT Services		WAGO Protocol	Native MQTT	Sparkplug payload B		
Service enabled	X	X	X	X	X	X						
Cloud platform	X	X	X	X	X	X						
Hostname	X	X	X	X	X	X						
Group ID			>		>					X		
Device ID	X	X										
Client ID			>	>	>	X		X	X			
Edge Node ID			>		>					X		
Activation Key	X	X										
Clean Session			X	(X)	(X)	X						
TLS			X	X	(X)	X						
Port			X	X	(X)	X						
CA file			X	X	X	X						
User			X	X								
Password			X	X								
Certification file			X		X	X						
Key file			X		X	X						
Use websockets	X	X										
Use compression	X	X	>					X	X			
Data Protocol			X	X	X	(X)						
• WAGO Protocol			X	X	X							
• Native MQTT			X	X	X	(X)						
• Sparkplug payload B			X		X							
Cache mode	X	X	X	X	X	X						
Last Will			X	X	X	X						
Last Will Topic			>	>	>	>						X
Last Will Message			>	>	>	>						X
Last Will QoS			>	>	>	>						X
Last Will Retain			>	>	(>)	>						X
Device info		X	>	>	>			X				
Device status		X	>	>	>			X				
Standard commands		X	>		>			X				

X: Visible and active

(X): Visible, but not active

>: Visible and active; dependent on other settings

(>): Visible, but not active; dependent on other settings

7.8.1.34 “Configuration of General SNMP Parameters” Page

The general settings for SNMP are given on the “Configuration of General SNMP Parameters” page.

7.8.1.34.1 “General SNMP Configuration” Group

Table 102: 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).

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!

7.8.1.35 “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.

7.8.1.35.1 “SNMP v1/v2c Manager Configuration” Group

Table 103: WBM “Configuration of SNMP v1/v2c Parameters” Page – “SNMP v1/v2c Manager Configuration” Group

Parameter	Explanation
Protocol enabled	It is displayed the SNMP protocol for v1/v2c is activated. The local community name is deleted when the protocol is deactivated.
Local Community Name	Specify here 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 **[Change]** to apply 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!

7.8.1.35.2 “Actually Configured Trap Receivers” Group(s)

Table 104: WBM “Configuration of SNMP v1/v2c Parameters” Page – “Actually Configured Trap Receivers” Group

Parameter	Explanation
Count	This displays number of configured trap receivers.

7.8.1.35.3 “Trap Receiver n” Group(s)

A dedicated group with the following information is displayed for each trap receiver:

Table 105: WBM “Configuration of SNMP v1/v2c Parameters” Page – “Trap Receiver n” Group(s)

Parameter	Explanation
IP Address	The IP address for the trap receiver (management station) is displayed here.
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).

Click **[Delete]** to delete the trap receiver. 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!

7.8.1.35.4 “Add New Trap Receiver” Group

You can enter 10 trap receivers.

Table 106: WBM “Configuration of SNMP v1/v2c Parameters” Page – “Add New Trap Receiver” Group

Parameter	Explanation
IP Address	Specify the IP address for the new trap receiver (management station) here.
Community Name	Specify here 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 **[Add]** to add a new trap receiver. 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!

7.8.1.36 “Configuration of SNMP v3 Users” Page

The general settings for SNMP v3 are shown on the “Configuration of SNMP v3 Users” page.

7.8.1.36.1 “Actually Configured v3 Users” Group(s)

Table 107: WBM “Configuration of SNMP v3” Page – “Actually Configured v3 Users” Group

Parameters	Explanation
Count	The number of configured v3 users is displayed.

7.8.1.36.2 “v3 User n” Group(s)

A group with the following information is displayed for each user:

Table 108: WBM “Configuration of SNMP v3 Users” Page – “v3 User n” Group(s)

Parameters	Explanation
Security Authentication Name	The user name is displayed.
Authentication Type	The authentication type for the SNMP v3 packets is displayed here. 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 here. 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 here. If nothing is displayed here, the “authentication key” is automatically used.
Notification Receiver IP	The IP address of a trap receiver for v3 traps is displayed here. If no v3 traps are to be sent for this user, this field remains blank.

Click **[Delete]** to delete the user. 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!

7.8.1.36.3 “Add New v3 User” Group

You can enter 10 users.

Table 109: WBM “Configuration of SNMP v3 Users” Page – “Add New v3 User” Group

Parameters	Explanation
Security Authentication Name	Enter the user name here. This name must be unique; a pre-existing user name is not accepted when entered here. 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	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. eight char.)	Specify the authentication key here. 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	Specify the encryption algorithm for the SNMP message here. Possible values: - No encryption (“None”) - Data Encryption Standard (“DES”) - Advanced Encryption Standard (“AES”)
Privacy Key (min. eight char.)	Enter the key for encryption of the SNMP message here. If nothing is specified here, the “authentication key” is automatically used. 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.
Notification Receiver IP	Specify an IP address for a trap receiver for v3 traps here. If no v3 traps are to be sent for this user, this field remains blank.

Click **[Add]** to add a new user. 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!

7.8.1.37 “Diagnostic Information” Page

The settings for displaying diagnostic messages are shown on the “Diagnostic Information” page.

Table 110: WBM “Diagnostic Information” Page

Parameter	Explanation
Read all notifications	Activate display of all messages.
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 cycle (sec)	Select the check box 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.

To refresh the display or to enable cyclic refresh, click the **[Refresh]** button. This button is only visible if the cyclic refresh is not enabled or stopped.

To enable cyclic refresh, click the **[Start]** button. The button is only visible if cyclic refresh is enabled and has not yet started.

To stop cyclic refresh again, click the **[Stop]** button. The button is only visible if cyclic refresh is enabled.

The cyclical update is performed for as long as the “Diagnostic Information” page is opened. If you change the WBM page, the update is stopped until you call up the “Diagnostic Information” Page again.

The messages are displayed below the settings.

7.8.1.38 "Configuration of General BACnet" Page

On the page "Configuration of General BACnet" you can make specific settings for the fieldbus BACnet.

7.8.1.38.1 "BACnet Status" Group

Table 111: WBM "Configuration of General BACnet" Page" – "BACnet Status" Group

Parameters	Explanation
Device-ID	Here the current device ID of the controller is displayed.

7.8.1.38.2 "BACnet General Parameter" Group

This group contains basic settings for the fieldbus.

Table 112: WBM "Configuration of General BACnet" Page" – "BACnet General Parameter" Group

Parameters	Explanation
Port Number	Here you set the communication port of the BACnet fieldbus.
Who-Is online interval time (sec)	Here you set the intervals at which "who-is" requests are sent from the device (minimum: 60).
Delete Persistence Data	The next time you restart, the persistent BACnet data is deleted.
Reset all BACnet Data and Settings to Default	The next time you restart, the BACnet-specific settings and data are reset to factory settings.

To apply a setting, click the **[Submit]** button.

The changes are usually only accepted after a restart of the stack/controller. For this use the reboot function of the WBM. Do not turn off the controller too soon!

7.8.1.38.3 "BACnet Upload" Group

Table 113: WBM "Configuration of General BACnet" Page" – "BACnet Upload" Group

Parameters	Explanation
New override.xml	Here you exchange an uploaded override file.

To select a file on the controller or PC, click the **[Browse]** button.

To transfer the selected file from the PC to the controller, click the **[Start Upload]** button.

To delete the existing file from the controller, click the **[Delete]** button.

The changes are usually only accepted after a restart of the stack/controller. For this use the reboot function of the WBM. Do not turn off the controller too soon!

7.8.1.39 “Configuration of BACnet Storage Location parameters” Page

On the page "Configuration of BACnet Storage Location parameters" you can make settings for the storage of BACnet specific parameters.

7.8.1.39.1 “BACnet Persistence” Group

This group offers the possibility of selecting the storage location (SD Card/ Internal Flash) to store the persistence data.

When the persistence settings are changed, a pop-up window alerts you to data loss until the next persistence completes.

Table 114: WBM “Configuration of BACnet Storage Location parameters” page – “BACnet Persistence” Group

Parameters	Explanation	
Storage location	Here you select the location for the persistence data. The selection is only possible if both memories are present.	
	Internal-Flash	The data is stored in the internal memory of the controller.
	SD-Card	The data is stored on the memory card. If "SD Card" is selected but the memory card is no longer plugged in, then this option is no longer active and only "Internal Flash" can be selected.

Changes are accepted without a restart.

7.8.1.39.2 “BACnet Trendlog“ Group

This group offers the possibility to select in which memory location (SD card/Internal Flash) the trendlog data is stored.

Table 115: WBM “Configuration of BACnet Storage Location parameters” page – “BACnet Trendlog” Group

Parameters	Explanation	
Storage location	Here you select the location for the trendlog data. The selection is only possible if both memories are present.	
	Internal-Flash	The data is stored in the internal memory of the controller.
	SD-Card	The data is stored on the memory card. If "SD Card" is selected but the memory card is no longer plugged in, then this option is no longer active and only "Internal Flash" can be selected.

Changes are accepted without a restart.

7.8.1.39.3 “BACnet Eventlog“ Group

This group offers the possibility to select in which memory location (SD card/Internal Flash) the eventlog data is stored.

Table 116: WBM “Configuration of BACnet Storage Location parameters” page – “BACnet Eventlog” Group

Parameters	Explanation	
Storage location	Here you select the location for the eventlog data. The selection is only possible if both memories are present.	
	Internal-Flash	The data is stored in the internal memory of the controller.
	SD-Card	The data is stored on the memory card. If "SD Card" is selected but the memory card is no longer plugged in, then this option is no longer active and only "Internal Flash" can be selected.

Changes are accepted without a restart.

7.8.1.40 “BACnet Diagnostic Information” Page

The "BACnet Diagnostic Information" page contains the settings for displaying the diagnostic messages.

Table 117: WBM “BACnet Diagnostic Information” page

Parameters	Explanation
Read all notifications	Here you switch on the display of all messages.
Read only the last n	Here you can switch on the display of the last n messages. Here you also enter the number of displayed messages.
Automatic refresh cycle (sec)	Select the check box to enable the cyclic update. Enter the cycle time in seconds with which a cyclic update is performed. Depending on the status, the label of the button changes ("Refresh"/"Start"/"Stop").

To refresh the display or activate the cyclic update, click the **[Refresh]** button. This button is only visible if the cyclic update is not switched on or stopped.

To activate the cyclical update, click the **[Start]** button. This button is only visible if the cyclic activation has been switched on and not yet started.

To stop the cyclical update, click the **[Stop]** button. This button is only visible when the cyclic update is active.

The cyclical update is only performed as long as the page "BACnet Diagnostic Information" is opened. When you switch to another WBM page, the update pauses until you return to the "BACnet Diagnostic Information" page.

The messages are displayed below the settings.

7.8.1.41 “Configuration of OpenVPN and IPsec” Page

The general settings for OpenVPN and IPsec are shown on the “Configuration of OpenVPN and IPsec” page.

7.8.1.41.1 “OpenVPN” Group

Table 118: WBM “Configuration of OpenVPN and IPsec” Page – “OpenVPN” Group

Parameters	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 controller or vice versa.	

To apply a status change, click the **[Submit]** button.

To select a file on the controller or PC, click the **[Browse]** button.

To transfer the selected file from the PC to the controller, click **[Start Upload]** button.

To transfer the selected file from the controller to the PC, click **[Start Download]** button.

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!

7.8.1.41.2 “IPsec” Group

Table 119: WBM “Configuration of OpenVPN and IPsec” Page – “IPsec” Group

Parameters	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.config	Select an IPsec configuration file to be transferred from PC to controller or vice versa.	
ipsec.secrets	Select an IPsec configuration file to be transferred from PC to controller.	

To apply a status change, click the **[Submit]** button.

To select a file on the controller or PC, click the **[Browse]** button.

To transfer the selected file to the controller, click **[Start Upload]** button.

To transfer the selected file from the controller to the PC, click **[Start Download]** button.

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!

7.8.1.41.3 “Certificate Upload” Group

Table 120: WBM “Configuration of OpenVPN and IPsec” Page – “Certificate Upload” Group

Parameters	Explanation
New Certificate	Select an certificate for transfer from a PC to the controller.
New Private Key	Select a key for transfer from a PC to the controller.

To select a file on the PC, click the **[Browse]** button.

To transfer the selected file to the controller, click **[Start Upload]** button. The changes will be effective immediately.

The certificates are saved in the directory “/etc/certificates/” and the keys in the directory “/etc/certificates/keys/”.

7.8.1.41.4 “Certificate List” Group

Table 121: 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.

Click **[Delete]** to delete an entry. The changes will be effective immediately.

7.8.1.41.5 “Private Key List” Group

Table 122: WBM “Configuration of OpenVPN and IPsec” Page – “Private Key List” Group

Parameters	Explanation
<key name>	The loaded keys are displayed. If no keys has been loaded. “No keys existing” is displayed.

Click **[Delete]** to delete an entry. The changes will be effective immediately.

7.8.1.42 “Security Settings” Page

The network security settings are found on the “Security Settings” page.

7.8.1.42.1 “Transport Layer Security Settings” Group

Table 123: “Security Settings” WBM Page – “Transport Layer Security Settings” Group

Parameters	Explanation	
TLS configuration	Here 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 on **[Submit]** to accept the changes. The changes will be effective immediately.



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.”

7.8.1.43 “Advanced Intrusion Detection Environment (AIDE) Page”

The network security settings are available on the “Advanced Intrusion Detection Environment (AIDE)” page.

7.8.1.43.1 “Run AIDE check at startup” Group

Table 124: “Advanced Intrusion Detection Environment (AIDE) WBM 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.

7.8.1.43.2 “Control AIDE and show log” Group

Table 125: “Advanced Intrusion Detection Environment (AIDE)” WBM 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 all notifications	Activate display of all messages.
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 cycle (sec)	Select the check box to enable cyclic refresh. Enter the cycle time in seconds in which a cyclic refresh is performed. The label of the button (“Refresh”/“Stop”) changes depending on status.

To refresh the display or to enable cyclic refresh, click the **[Refresh]** button. The button is only visible if cyclic refresh is enabled and has not yet started.

To stop cyclic refresh again, click the **[Stop]** button. The button is only visible if cyclic refresh is enabled.

The cyclical update is performed for as long as the “Advanced Intrusion Detection Environment (AIDE)” page is opened. If you change the WBM page, the update is stopped until you call up the “Advanced Intrusion Detection Environment (AIDE)” page again.

7.8.1.44 “Open Source Licenses” Page

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

7.8.1.45 “WAGO Licenses” Page

The licence conditions for the WAGO software used in the controller are listed on the “WAGO Licenses” page.

7.8.2 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 ETHERNET interface X1 of the controller using a 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.

Alternatively, you can also connect the controller via a serial interface:

1. Connect a PC to the X3 serial interface of the controller using a terminal program.
2. Start the terminal program.
3. Select "Serial" as the connection type and enter a baud rate of 115200 bauds as the connection parameter. The settings for data bits, stop bits and parity do not need to be adjusted.
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 34: CBM main menu (example)

7.8.2.1 CBM Menu Structure Overview

Table 126: 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 126: CBM Menu Structure

Menu Hierarchy	
1. Users	
2. Create Image	
3. Owner of Serial Interface	
4. 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.

7.8.2.2 “Information” Menu

This menu contains other submenus with information on the controller and network.

Table 127: “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]**.

7.8.2.2.1 “Information” > “Controller Details” Submenu

In this submenu, the controller properties are displayed.

Table 128: “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]**.

7.8.2.2.2 “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 129: “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]**.

7.8.2.3 “PLC Runtime” Menu

This menu contains other submenus with information and settings for the runtime system.

Table 130: “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]**.

7.8.2.3.1 “PLC Runtime” > “Information” Submenu

This submenu contains other submenus with information on the runtime system and PLC program.

Table 131: “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]**.

7.8.2.3.2 “Information” > “Runtime Version” Submenu

In this submenu, the runtime version is displayed.

Table 132: “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]**.

7.8.2.3.3 “PLC Runtime” > “General Configuration” Submenu

This submenu contains other submenus with general settings for the runtime system.

Table 133: “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]**.

7.8.2.3.4 “General Configuration” > “PLC Runtime Version” Submenu

In this submenu, select which PLC runtime system is enabled.

Table 134: “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]**.

7.8.2.3.5 “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 135: “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]**.

7.8.2.3.6 “PLC Runtime” > “WebVisu” Submenu

This submenu contains information and settings for the Web visualization.

Table 136: “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]**.

7.8.2.4 “Networking” Menu

This menu contains other submenus with settings for the network configuration.

Table 137: “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]**.

7.8.2.4.1 “Networking” > “Host/Domain Name” Submenu

This submenu contains the “Hostname” and “Domain Name” submenu with setting options for the general TCP/IP parameters.

Table 138: “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]**.

7.8.2.4.2 “Host/Domain Name” > “Hostname” Submenu

In this submenu, you can set the hostname of the controller.

Table 139: “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.

7.8.2.4.3 “Host/Domain Name” > “Domain Name” Submenu

In this submenu, you can set the domain name of the controller.

Table 140: “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.

7.8.2.4.4 “Networking” > “TCP/IP” Submenu

This submenu contains other submenus with the TCP/IP settings for the ETHERNET interfaces.

Table 141: “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**].

7.8.2.4.5 “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 142: “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]**.

7.8.2.4.6 “IP Address” > “Xn” Submenu

This submenu contains the settings for the selected interface.

Table 143: “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.

7.8.2.4.7 “TCP/IP” > “Default Gateway” Submenu

This submenu contains other submenus with settings for the default gateway.

Table 144: “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]**.

7.8.2.4.8 “Default Gateway” > “Default Gateway n” Submenu

This submenu contains the settings for the selected gateway.

Table 145: “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.

7.8.2.4.9 “TCP/IP” > “DNS Server” Submenu

This submenu contains the settings for the DNS server.

Table 146: “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.

7.8.2.4.10 “Networking” > “Ethernet” Submenu

This submenu contains other submenus with settings for the ETHERNET configuration.

Table 147: “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 IP address(es)
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]**.

7.8.2.4.11 “Ethernet” > “Switch Configuration” Submenu

This submenu contains the settings for the Switch configuration.

Table 148: “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]**.

7.8.2.4.12 “Ethernet” > “Ethernet Ports” Submenu

This submenu contains other submenus with settings for the ETHERNET interfaces.

Table 149: “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]**.

7.8.2.4.13 “Ethernet Ports” > “Interface Xn” Submenu

This submenu contains the settings for the selected ETHERNET interface.

Table 150: “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]**.

7.8.2.5 “Firewall” Menu

This menu contains other submenus for the firewall functionality settings.

Table 151: “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]**.

7.8.2.5.1 “Firewall” > “General Configuration” Submenu

This submenu contains the general settings for the firewall.

Table 152: “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.

7.8.2.5.2 “General Configuration” > “Interface xxx” Submenu

This submenu contains the firewall settings on the IP level for the selected interface.

Table 153: “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.

7.8.2.5.3 “Firewall” > “MAC Address Filter” Submenu

This submenu contains the settings for the MAC address filter.

Table 154: “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]**.

7.8.2.5.4 “MAC Address Filter” > “MAC address filter whitelist” Submenu

This submenu displays all available filter entries.

Table 155: “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]**.

7.8.2.5.5 “MAC address filter whitelist” > “Add new / No (n)” Submenu

In this submenu, you can create, change or delete filter entries.

Table 156: “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.

7.8.2.5.6 “Firewall” > “User Filter” Submenu

This submenu displays all available filter entries.

Table 157: “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]**.

7.8.2.5.7 “User Filter” > “Add New / No (n)” Submenu

In this submenu, you can create, change or delete filter entries.

Table 158: “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.

7.8.2.6 “Clock” Menu

This menu contains other submenus for the date and time settings.

Table 159: “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.

7.8.2.7 “Administration” Menu

This menu contains settings for controller administration.

Table 160: “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. Owner of Serial Interface	Select the serial interface assignment.	
	0. Back to ...	Back to the higher-level menu
	1. Linux Console	The serial interface is assigned to the Linux® console.
	2. Un-assigned	The serial interface is not assigned and is available for applications or CODESYS.
4. 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]**.

7.8.2.7.1 “Administration” > “Users” Submenu

This submenu contains settings for the user passwords.

Table 161: “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.

7.8.2.7.2 “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 162: “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.

7.8.2.8 “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 163: “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]**.

7.8.2.8.1 “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 164: “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.

7.8.2.8.2 “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 165: “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.

7.8.2.8.3 “Firmware Backup” > “Destination” Submenu

This submenu contains a selection option for the backup destination drive.

Table 166: “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.

7.8.2.8.4 “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 167: “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.

7.8.2.8.5 “Firmware Restore” > “Select Package” Submenu

This submenu contains a selection option for the data to be restored.

Table 168: “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.

7.8.2.8.6 “Package Server” > “System Partition” Submenu

This submenu contains information and setting options for the current system partition.

Table 169: “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]**.

7.8.2.9 “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 170: “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]**.

7.8.2.9.1 “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 171: “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.

7.8.2.10 “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.

7.8.2.11 “Ports and Services” Menu

This submenu contains other submenus with settings for the respective services.

Table 172: “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]**.

7.8.2.11.1 “Ports and Services” > “Telnet” Submenu

This submenu contains the settings for the Telnet service.

Table 173: “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]**.

7.8.2.11.2 “Ports and Services” > “FTP” Submenu

This submenu contains the settings for the FTP service.

Table 174: “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]**.

7.8.2.11.3 “Ports and Services” > “FTPS” Submenu

This submenu contains the settings for the FTPS service.

Table 175: “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]**.

7.8.2.11.4 “Ports and Services” > “HTTP” Submenu

This submenu contains the settings for the HTTP service.

Table 176: “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]**.

7.8.2.11.5 “Ports and Services” > “HTTPS” Submenu

This submenu contains the settings for the HTTPS service.

Table 177: “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]**.

7.8.2.11.6 “Ports and Services” > “NTP” Submenu

This submenu contains the settings for the NTP service.

Table 178: “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.

7.8.2.11.7 “Ports and Services” > “SSH” Submenu

This submenu contains the settings for the SSH service.

Table 179: “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]**.

7.8.2.11.8 “Ports and Services” > “TFTP” Submenu

This submenu contains the settings for the TFTP service.

Table 180: “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.

7.8.2.11.9 “Ports and Services” > “DHCPD” Submenu

This submenu contains the settings for the DHCPD service.

Table 181: “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]**.

7.8.2.11.10 “DHCPD” > “Xn” Submenu

This submenu contains the settings for the DHCPD service for the selected interface.

Table 182: “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.

7.8.2.11.11 “Ports and Services” > “DNS” Submenu

This submenu contains the settings for the DNS service.

Table 183: “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.

7.8.2.11.12 “Ports and Services” > “IOCHECK PORT” Submenu

This submenu contains settings for the WAGO-I/O-CHECK port.

Table 184: “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]**.

7.8.2.11.13 “Ports and Services” > “Modbus TCP” Submenu

This submenu contains the settings for the Modbus TCP service.

Table 185: “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]**.

7.8.2.11.14 “Ports and Services” > “Modbus UDP” Submenu

This submenu contains the settings for the Modbus UDP service.

Table 186: “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]**.

7.8.2.11.15 “Ports and Services” > “OPC UA” Submenu

This submenu contains the settings for the OPC UA service.

Table 187: “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]**.

7.8.2.11.16 “...” > “Firewall Status” Submenu

This submenu contains firewall settings for the selected service.

Table 188: “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]**.

7.8.2.11.17 “Ports and Services” > “PLC Runtime Services” Submenu

This submenu contains the settings for the PLC runtime system services.

Table 189: “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 <i>e!RUNTIME</i>
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.

7.8.2.11.18 “PLC Runtime Services” > “e!RUNTIME” Submenu

This submenu contains the settings for the *e!RUNTIME* service.

Table 190: “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 <i>e!RUNTIME</i> 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]**.

7.8.2.12 “SNMP” Menu

This menu contains other submenus with the SNMP settings.

Table 191: “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]**.

7.8.2.12.1 “SNMP” > “General SNMP Configuration” Submenu

This submenu contains the general SNMP settings.

Table 192: “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.

7.8.2.12.2 “SNMP” > “SNMP v1/v2c Manager Configuration” Submenu

This submenu contains the SNMP v1/v2c Manager settings.

Table 193: “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.

7.8.2.12.3 “SNMP” > “SNMP v1/v2c Trap Receiver Configuration” Submenu

This submenu contains settings for the v1/v2c trap receivers.

Table 194: “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	<p>Opens a series of submenus to create a new v1/v2c trap receiver</p> <p>You can enter 10 trap receivers.</p> <p>The following entries/selections are possible:</p> <ul style="list-style-type: none"> • 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.

7.8.2.12.4 “SNMP” > “SNMP v3 Configuration” Submenu

This submenu contains settings for SNMP v3.

Table 195: “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	<p>Opens a series of submenus to create a new v3 user</p> <p>You can enter 10 users.</p> <p>The following entries/selections are possible:</p> <ul style="list-style-type: none"> • 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.

7.8.2.12.5 “SNMP” > “(Secure)SNMP firewalling” Submenu

These submenus contain the SNMP firewall settings.

Table 196: “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]**.

7.8.3 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 correct COM port after starting “WAGO Ethernet Settings”.

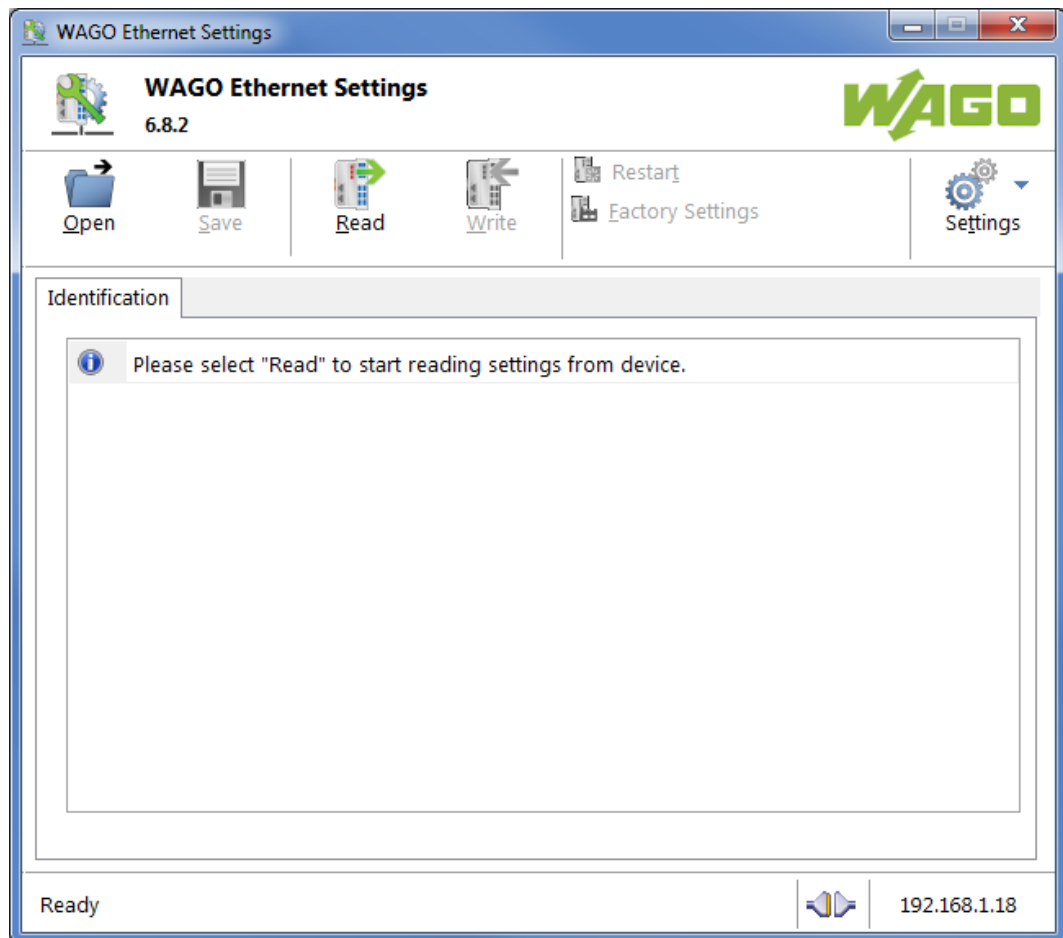


Figure 35: “WAGO Ethernet Settings” – Start Screen

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

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

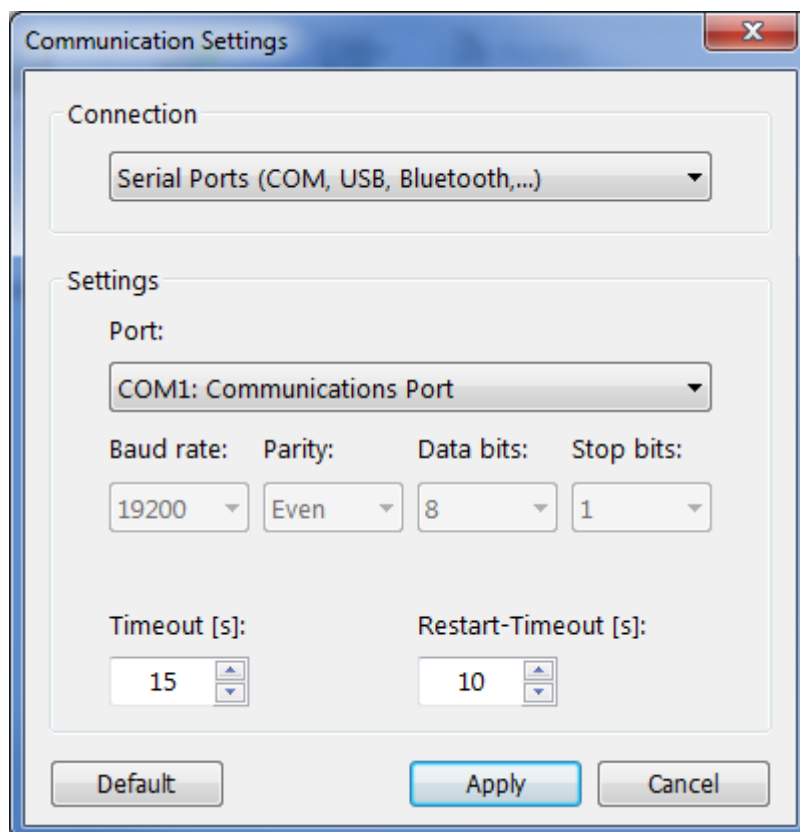


Figure 36: "WAGO Ethernet Settings" – Communication Link

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]**.

7.8.3.1 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.

Identification	Network	PLC	Status
Item Number	750-8206		
Description	WAGO 750-8206 PFC200 CS 2ETH RS CAN DPS		
FW Version	02.06.20(09)		
HW Version	01		
FWL Version	2014.11.0-pXc-02.01.01 IDX=02		
Serial Number	SN20141204T134141-0025639#PFC 0030DE400E6F		
MAC address X1	0030DE400E6F		
MAC address X2	0030DE400E6F		
IP address X1	192.168.1.18 (Static Configuration)		
IP address X2	0.0.0.0 (No configuration!)		
Runtime system	e!RUNTIME		

Figure 37: “WAGO Ethernet Settings” – Identification Tab (Example)

7.8.3.2 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.

Parameter	Edit	Currently used
Address Source	Static Configuration	Static Configuration
IP address	192.168.1.18	192.168.1.18
Subnet Mask	255.255.255.0	255.255.255.0
Gateway	0.0.0.0	0.0.0.0
Preferred DNS-Server	0.0.0.0	0.0.0.0
Alternative DNS-Server	0.0.0.0	0.0.0.0
Time Server	0.0.0.0	0.0.0.0
Hostname		PFC200-400E6F
Domain name	localdomain.lan	localdomain.lan

Interface X₁

Interface X₂

Run WBM

Interfaces

☐ Switched

☒ Separated

Figure 38: “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.

7.8.3.3 PLC Tab

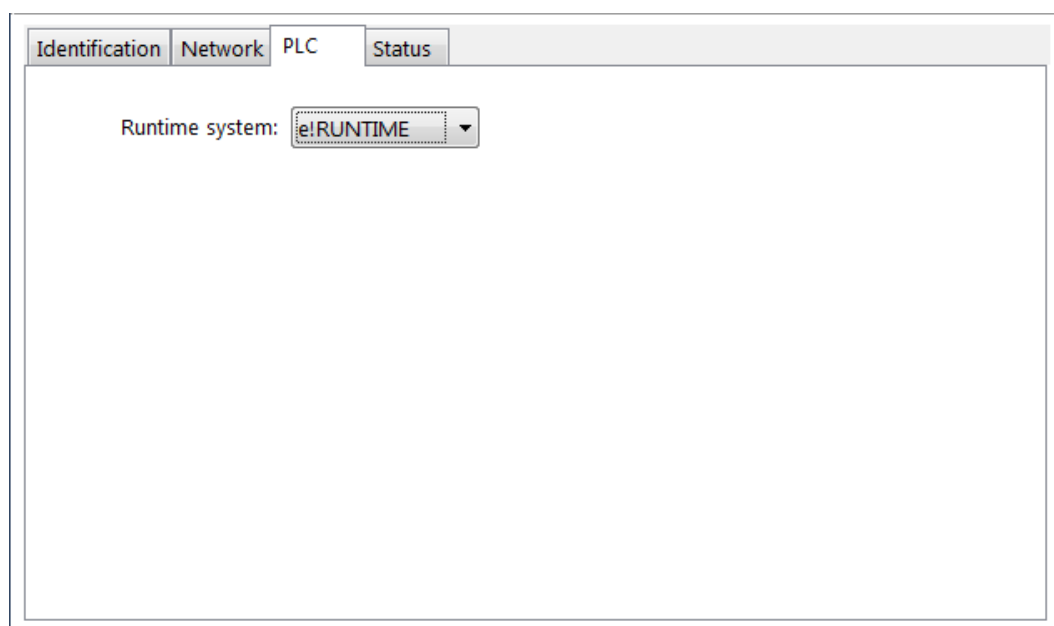


Figure 39: "WAGO Ethernet Settings" – Protocol Tab

Here you can select the runtime system.

7.8.3.4 Status Tab

The screenshot displays the 'WAGO Ethernet Settings' window with the 'Status' tab selected. The window has a tabbed interface with four tabs: 'Identification', 'Network', 'PLC', and 'Status'. The 'Status' tab is active and contains two main sections:

- Status:** A list of five checkboxes:
 - ☒ Field bus active
 - ☒ Write access enabled
 - ☐ Monitor-Mode enabled
 - ☐ Control-Mode enabled
 - ☐ Factory test mode enabled
- Blink code:** A section displaying error information:
 - Error code: 0
 - Argument: 0
 - No Error

Figure 40: "WAGO Ethernet Settings" – Status Tab

General information about the controller status is displayed here.

8 **e!RUNTIME Runtime Environment**

8.1 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.

8.2 CODESYS V3 Priorities

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

Table 197: 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

8.3 Memory Spaces under e!RUNTIME

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

- Program and data memory: 60 Mbytes
- Input data: 64 kbytes
- Output data: 64 kbytes
- Flags: 24 kbytes
- Retain: 104 kbytes
- Function block limitation: $12 * 4096 \text{ bytes} = 48 \text{ kbytes}$

8.3.1 Program and Data Memory

The program (also code) and data memory has a size of 60 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.

8.3.2 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., $4096 * 12$).

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.

8.3.3 Remanent Memory

A total of 128 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.

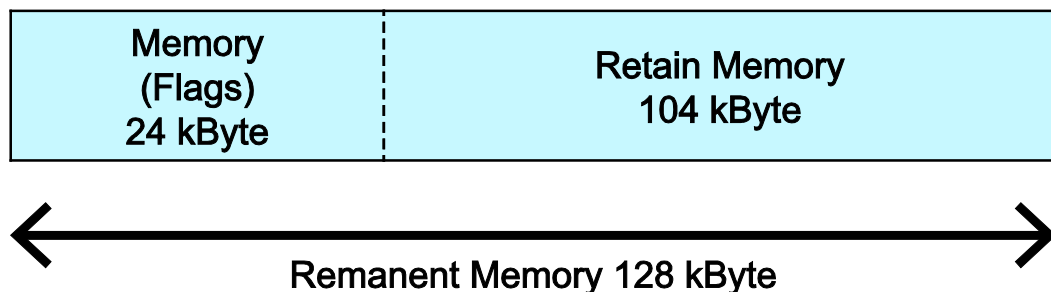


Figure 41: Remanent Main Memory

9 Modbus – e!RUNTIME

9.1 Modbus Address Overview

	Modbus® Register Access	Modbus® Bit Access
PFC-OUT Modbus®-IN Size: 32000 registers	0x0000	0x0000
	Only read access FC3, FC4, FC23, FC66	Only read access FC1, FC2 0x7FFF
	0x7CFF	
PFC-IN Modbus®-OUT Size: 32000 registers	0x7D00	0x8000
	Read and write access FC3, FC4, FC6, FC16, FC23, FC66	Read and write access FC1, FC2, FC5, FC15 0xFFFF
	0xF9FF	
Modbus® Special registers Size: 1536 registers	0xFA00	
	Read and write access FC3, FC4, FC6, FC16, FC23, FC66	
	0xFFFF	

Figure 42: Modbus Address Overview

9.2 Modbus Registers

Table 198: 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 198: 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.

9.2.1 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.

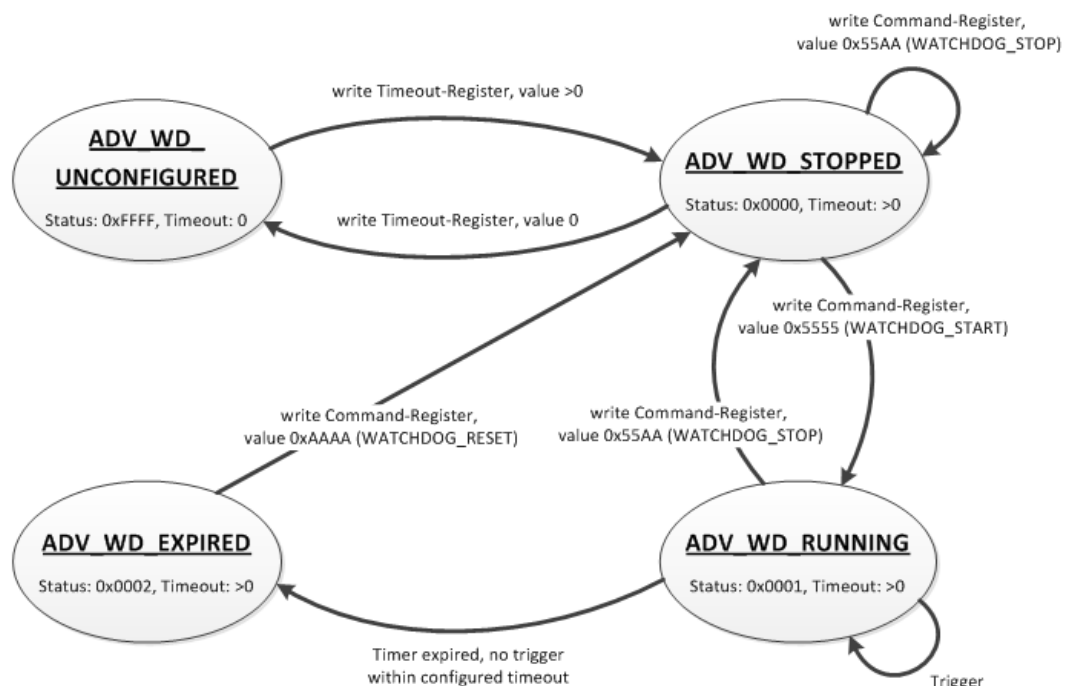


Figure 43: State Diagram, **ADVANCED_WATCHDOG** Operation Mode

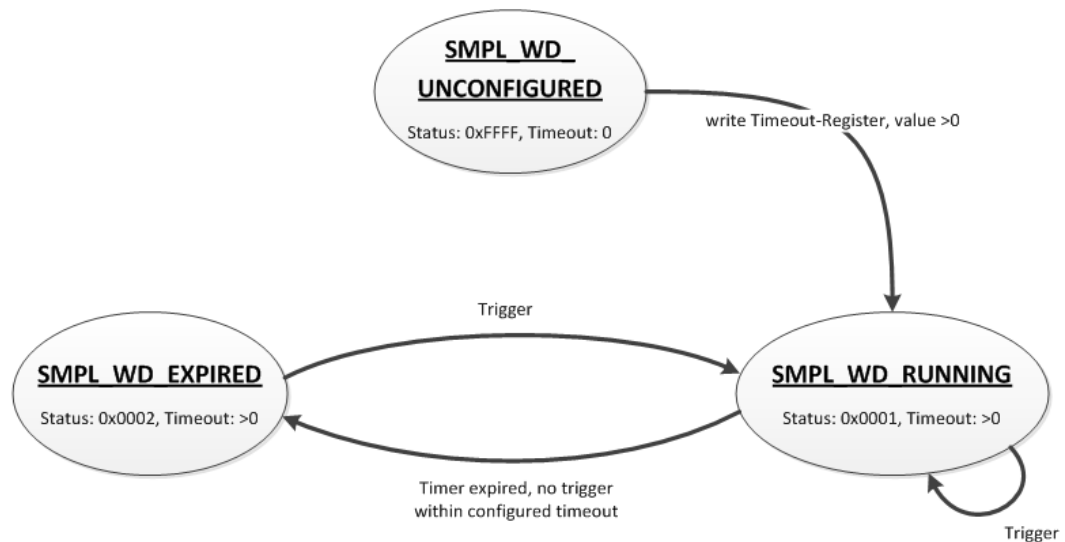


Figure 44: State Diagram, SIMPLE_WATCHDOG Operation Mode

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.

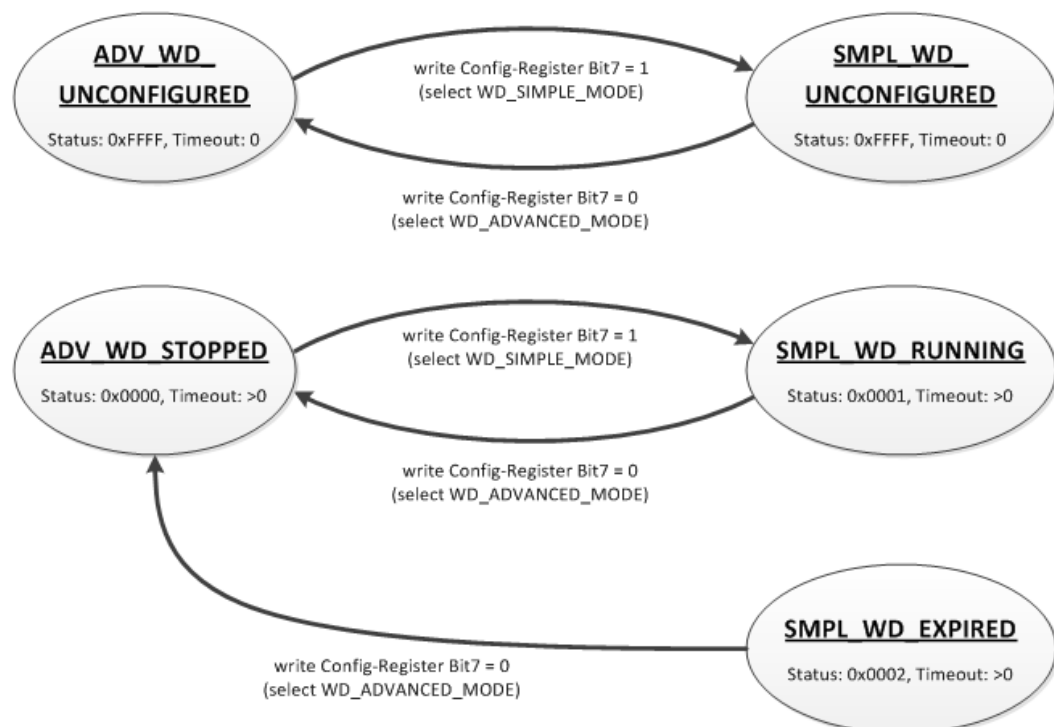


Figure 45: State Diagram, Switching Operation Modes

9.2.1.1 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 199: 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.

9.2.1.2 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.

9.2.1.3 Register 0xFA02 – Watchdog Status

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

Table 200: 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.

9.2.1.4 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 201: 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.

9.2.1.5 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.

9.2.2 Status Registers

9.2.2.1 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

9.2.3 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.

9.2.3.1 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

9.2.3.2 Firmware Version

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

9.2.3.3 Hardware Version

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

9.2.3.4 Firmware Loader/Boot Loader

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

9.2.4 Modbus Process Image Version

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

9.2.5 Modbus Process Image Registers

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

9.2.6 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

9.2.7 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.

9.3 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:

$$\text{cpu_load} = 800 \mu\text{s} / t_z * 100$$

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).

10 Diagnostics

10.1 Operating and Status Messages

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

10.1.1 Power Supply Indicating Elements

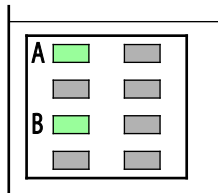


Figure 46: Power Supply Indicating Elements

The A LED (system power supply) indicates following diagnostics:

Table 202: System Power Supply Diagnostics

Status	Explanation	Solution
Green	24V system power supply voltage present	---
Off	No 24V system power supply voltage present	Switch on the power supply. Check the supply voltage.

The B LED (field-side power supply) indicates following diagnostics:

Table 203: Field-Side Supply Diagnostics

Status	Explanation	Solution
Green	24V field-side supply voltage present	---
Off	No 24V field-side supply voltage present	Switch on the power supply. Check the supply voltage.

10.1.2 Fieldbus/System Indicating Elements

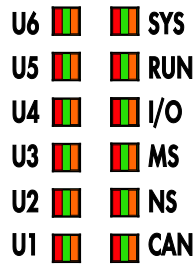


Figure 47: Indicating Elements for System/Fieldbus

The SYS LED indicates following diagnostics:

Table 204: 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	---
Orange/red flashing	No license; evaluation period not yet expired	The libraries or device functions affected are shown in e!COCKPIT . Activate the associated licenses before the evaluation period ends, or remove the libraries or device functions from your application. The device has unrestricted functionality until the evaluation period ends.
Red flashing	No license; evaluation period has expired	The libraries or device functions affected are shown in e!COCKPIT . Activate the associated licenses promptly, or remove the libraries or device functions from your application. Otherwise, the application can no longer be started after being downloaded again or started as a boot application after the device is restarted.

The RUN LED indicates following diagnostics:

Table 205: 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: <ul style="list-style-type: none"> - 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.

The I/O LED indicates following diagnostics:

Table 206: 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.

The MS LED indicates following diagnostics:

Table 207: 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."

The BT LED indicates following diagnostics:

Table 208: BT-LED Diagnostics

Status	Explanation	Remedy
Green	Fieldbus status Ok. Network initialization completed, BACnet stack started. Ready for fieldbus traffic.	---
Green flashing	Initialization BACnet stack.	1. Wait for the initialization to complete.
Red	The system displays an unrecoverable error.	1. Restart the controller by switching the supply voltage off and on. 2. If the error persists, contact WAGO I/O-Support.
Red flashing	Error initializing the BACnet stack. Incorrect configuration.	1. Correct the fieldbus configuration. 2. Check the BACnet diagnostics page in the WBM for information about the possible cause of the problem.
Off	There is no operating voltage for the system.	1. Check the voltage supply.
Yellow	e!Runtime Libs problems (e.g. no connection between e!Runtime object and BACnet object).	1. Check the BACnet configuration with the included BACnet objects and Your e!COCKPIT project for possible inconsistencies (e!COCKPIT objects in greater detail than in WBC).
Yellow flashing	Settings of the "Storage Location" changed in the WBM. <ul style="list-style-type: none"> Change of storage location until completely changed (applies in case of persistence). Storage on SD selected, but SD not available (trend/eventlog/persistence). 	1. Wait for the corresponding persistence time of 30 sec. Then the LED should change to green. Do not turn off the controller during this time, as data may be lost. 2. Insert an SD card into the controller and wait until the LED goes off.
Green/Red flashing	BACnet backup and restore mode active.	1. Wait for the BACnet Backup and Restore service to complete.
Green/Yellow flashing	BACnet overload.	1. Reduce potential BACnet requests from/to the controller.

10.1.3 Network Indicating Elements

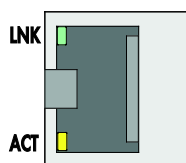


Figure 48: Indicating Elements, RJ-45 Jacks

The LNK LED indicates following diagnostics:

Table 209: LNK-LED Diagnostics

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

The ACT LED indicates following diagnostics:

Table 210: ACT-LED Diagnostics

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

10.2 Diagnostics Messages via Flashing Sequences

10.2.1 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.

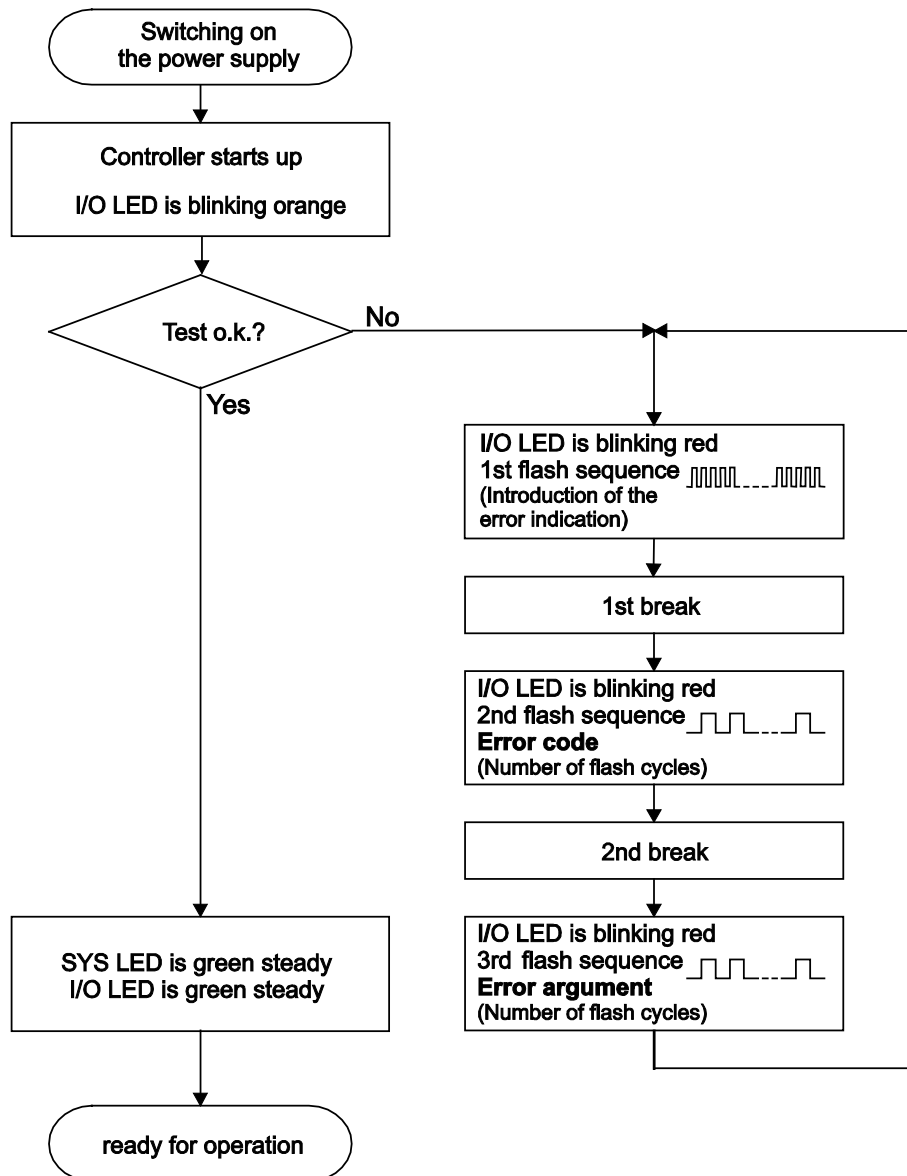


Figure 49: Flashing Sequence Process Diagram

10.2.2 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 1 Hz.
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.

10.2.3 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 211: 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 212: Error Code 1, Explanation of Blink Codes and Procedures for Troubleshooting

Error Argument	Cause	Remedy
-	Invalid parameter checksum for local bus interface	<ul style="list-style-type: none"> - 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.	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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.	<ul style="list-style-type: none"> - 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 212: Error Code 1, Explanation of Blink Codes and Procedures for Troubleshooting

Error Argument	Cause	Remedy
7	Error occurred while writing to the serial EEPROM	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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.	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - Switch off the power to the controller. - Reduce the number of I/O modules. - Then switch the power back on.

Table 213: Error Code 2, Explanation of Blink Codes and Procedures for Troubleshooting

Error Argument	Cause	Remedy
2	Maximum size of the process image exceeded	<ul style="list-style-type: none"> - Switch off the power to the controller. - Reduce the number of I/O modules. - Switch the power back on.

Table 214: 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	<p>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:</p> <ul style="list-style-type: none"> - 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). <p>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.</p> <ul style="list-style-type: none"> - 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 215: Error Code 4, Explanation of Blink Codes and Procedures for Troubleshooting

Error Argument	Cause	Solution
--	Maximum permissible number of I/O modules exceeded.	<ul style="list-style-type: none"> - 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.	<ul style="list-style-type: none"> - Switch off the power to the controller. - Replace the (n+1)th process data module. - Switch the power back on. <p>I/O modules that do not provide any data are ignored (e.g., supply module without diagnostics).</p>

Table 216: Error Code 5, Explanation of Blink Codes and Procedures for Troubleshooting

Error Argument	Cause	Solution
n*	Register communication error during local bus initialization	<ul style="list-style-type: none"> - Switch off the power to the controller. - Replace the (n+1)th process data module. - Switch the power back on. <p>I/O modules that do not provide any data are ignored (e.g., supply module without diagnostics).</p>

Table 217: 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.	<ul style="list-style-type: none"> - 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 218: 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 CODESYS applications: - Contact WAGO Support. For C applications: - Check the time monitoring settings.

10.2.4 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 219: Overview of MS-LED Error Codes

Error Code	Explanation
1	Configuration error

Table 220: 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	<ul style="list-style-type: none">- 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.

11 Service

11.1 Inserting and Removing the Memory Card

11.1.1 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.

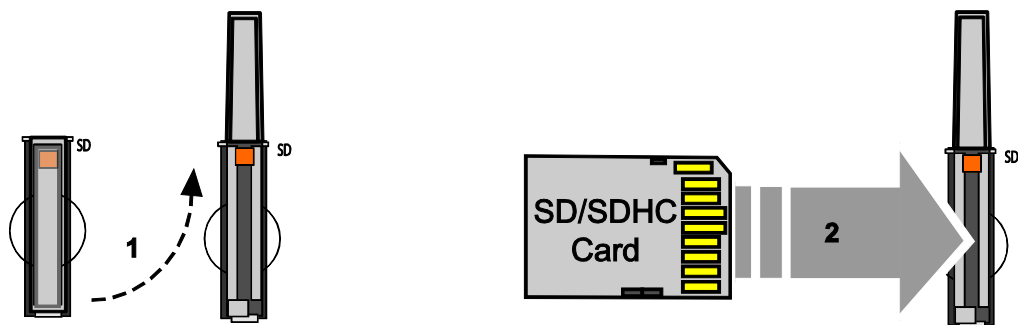


Figure 50: Inserting the Memory Card

11.1.2 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.

11.2 Firmware Changes



Note

Obtain documentation appropriate for the firmware target version!

A firmware upgrade or downgrade 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 an upgrade/downgrade.

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

11.2.1 Perform Firmware Upgrade

NOTICE

Do not switch the controller off!

The controller can be damaged by interrupting the upgrade process.

Do not switch the controller off during the upgrade process and do not disconnect the power supply!

Proceed as follows if you want to upgrade the controller to a later firmware version:

1. Save your application and the controller settings.
2. Switch off the controller.
3. Insert the memory card with the new firmware image into the memory card slot.
4. Switch on the controller.
5. After booting the controller, launch the WBM "Create Boot Image" page (you may have to temporarily change the IP address).
6. Create a new boot image on the internal memory.
7. Switch off the controller after completing the process.
8. Remove the memory card.
9. Switch on the controller.

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

11.2.2 Perform Firmware Downgrade

NOTICE

Do not switch the controller off!

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

Note

**Note the firmware version**

For devices with a factory installation of a firmware \geq FW 05, a simple downgrade to a version \leq FW 04 is not possible!
Use a special downgrade image.

Proceed as follows if you want to downgrade the controller to an earlier firmware version:

1. Save your application and the controller settings.
2. Switch off the controller.
3. Insert the memory card with the new firmware image into the memory card slot. Use a special downgrade image if necessary.
4. Switch on the controller.
5. After booting the controller, launch the WBM "Create Boot Image" page (you may have to temporarily change the IP address).
6. Create a new boot image on the internal memory.
7. Switch off the controller after completing the process.
8. Remove the memory card.
9. Switch on the controller.

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

11.2.3 Factory Reset

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



All parameters and passwords are overwritten!

All controller parameters and passwords are overwritten by a factory reset.
Stored boot projects are deleted, including existing web visualization data.
Subsequently installed firmware functions are not overwritten.
If you have any questions, contact WAGO Support.

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

11.3 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.

12 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.

12.1 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.

12.1.1 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.

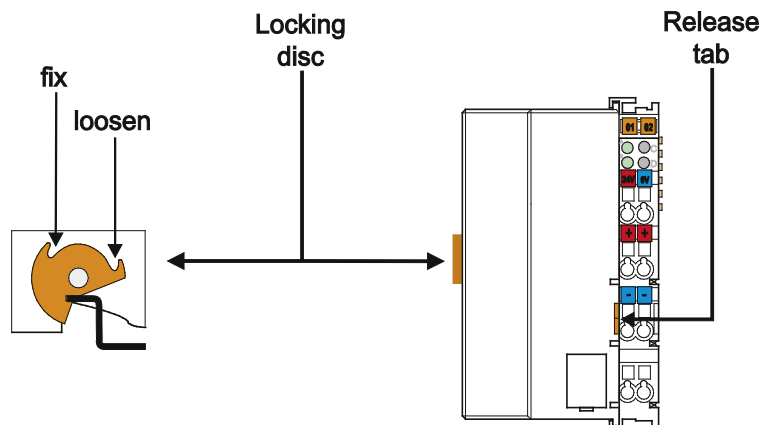


Figure 51: Release Tab of Controller

Note



Do not take the controller enclosure apart!

The enclosure sections are firmly joined. The feed-in section with the CAGE CLAMP® connections cannot be separated from the other enclosure section.

13 Disposal

13.1 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.

13.2 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.

14 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.

14.1 Marking Configuration Examples

14.1.1 Marking for Europe According to ATEX and IECEx

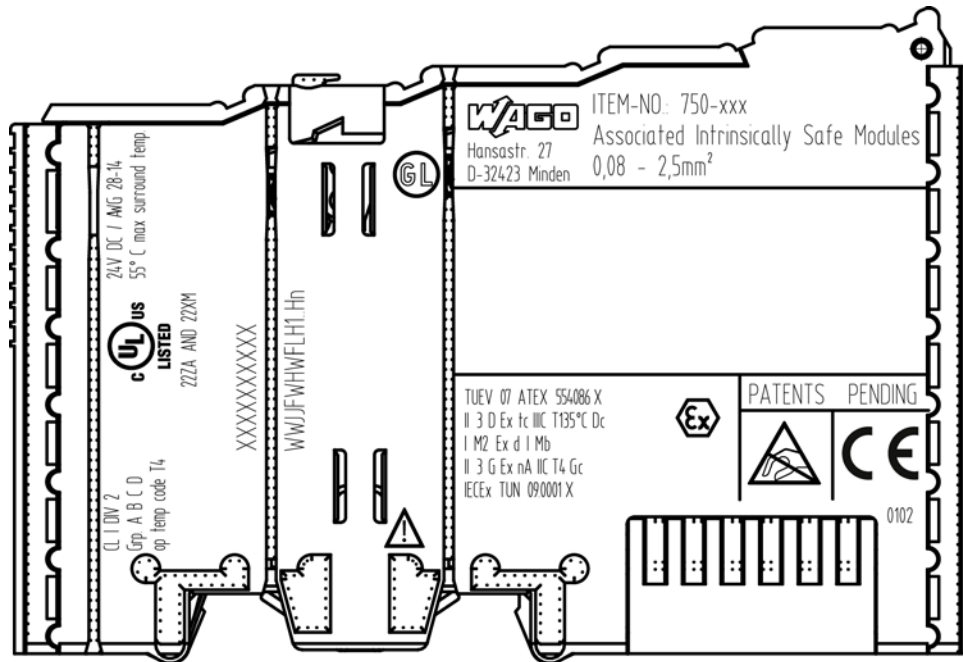


Figure 52: Marking Example According to ATEX and IECEx

TUEV 07 ATEX 554086 X
 II 3 D Ex tc IIC T135°C Dc
 I M2 Ex d I Mb
 II 3 G Ex nA IIC T4 Gc
 IECEx TUN 090001 X



Figure 53: Text Detail – Marking Example According to ATEX and IECEx

Table 221: 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)

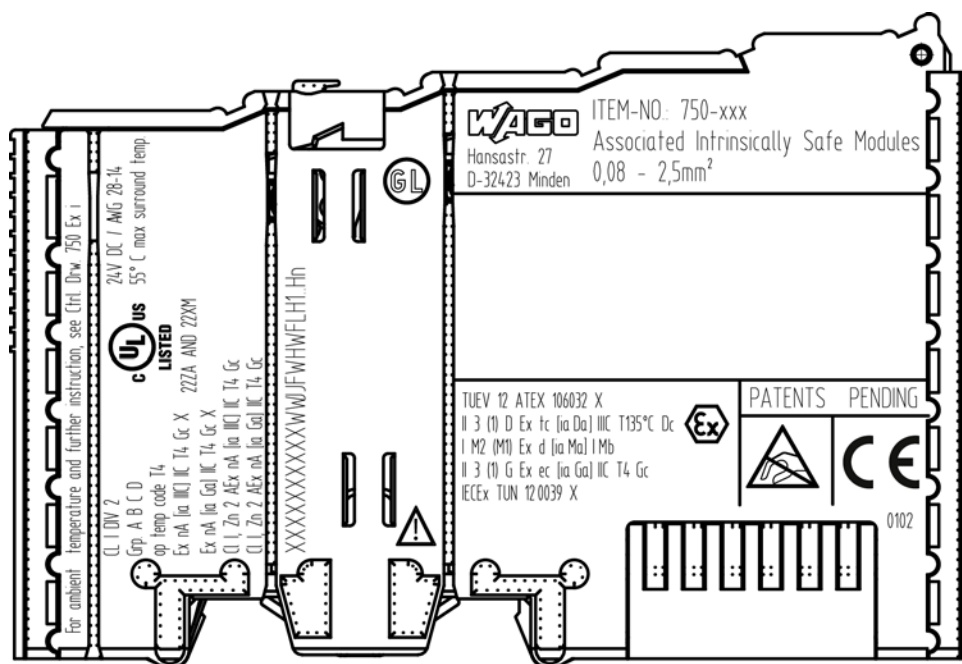


Figure 54: Marking Example for Approved Ex i I/O Module According to ATEX and IECEx

TUEV 12 ATEX 106032 X
 II 3 (1) D Ex tc [ia Da] IIC T135°C Dc
 I M2 (M1) Ex d [ia Ma] IMb
 II 3 (1) G Ex ec [ia Ga] IIC T4 Gc
 IECEx TUN 120039 X



Figure 55: Text Detail – Marking Example for Approved Ex i I/O Module According to ATEX and IECEx

Table 222: Description of Marking Example for Approved Ex i I/O Module 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)

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

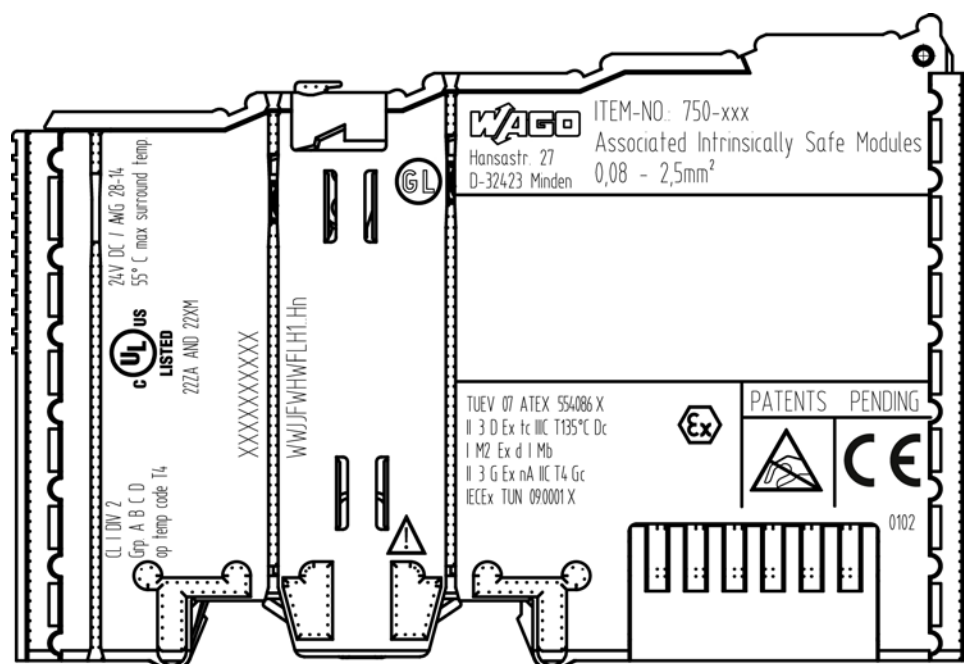


Figure 56: Marking Example According to NEC

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

Figure 57: Text Detail – Marking Example According to NEC 500

Table 223: 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

CI I, Zn 2 AEx nA [ia Ga] IIC T4 Gc

Figure 58: Text Detail – Marking Example for Approved Ex i I/O Module According to NEC 505

Table 224: Description of Marking Example for Approved Ex i I/O Module According to NEC 505

Marking	Description
CI 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)

CI I, Zn 2 AEx nA [ia IIIC] IIC T4 Gc

Figure 59: Text Detail – Marking Example for Approved Ex i I/O Module According to NEC 506

Table 225: Description of Marking Example for Approved Ex i I/O Modules According to NEC 506

Marking	Description
CI 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)

Ex nA [ia IIIC] IIC T4 Gc X

Ex nA [ia Ga] IIC T4 Gc X

Figure 60: Text Detail – Marking Example for Approved Ex i I/O Modules According to CEC 18 attachment J

Table 226: Description of Marking Example for Approved Ex i I/O Modules 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

14.2 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.

14.2.1 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 $0\text{ °C} \leq T_a \leq +55\text{ °C}$ or $-20\text{ °C} \leq T_a \leq +60\text{ °C}$ for components with extension number .../025-xxx or $-40\text{ °C} \leq T_a \leq +70\text{ °C}$ 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.

14.2.2 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.

15 Appendix

15.1 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!

15.1.1 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.

15.1.1.1 1 Channel Digital Input Module with Diagnostics

750-435

Table 227: 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

15.1.1.2 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 228: 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

15.1.1.3 2 Channel Digital Input Module with Diagnostics

750-419, -421, -424, -425,
753-421, -424, -425

Table 229: 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

15.1.1.4 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 230: 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

15.1.1.5 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 231: 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

15.1.1.6 8 Channel Digital Input Modules

750-430, -431, -436, -437, -1415, -1416, -1417, -1418,
753-430, -431, -434, -436, -437

Table 232: 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

15.1.1.7 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 233: 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	Signal status DI 7	Signal status DI 6	Signal status DI 5	Signal status DI 4	Signal status DI 3	Signal status DI 2	Signal status DI 1
Channel 8	Channel 7	Channel 6	Channel 5	Channel 4	Channel 3	Channel 2	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	Wire break /short circuit Data bit DI 7	Wire break /short circuit Data bit DI 6	Wire break /short circuit Data bit DI 5	Wire break /short circuit Data bit DI 4	Wire break /short circuit Data bit DI 3	Wire break /short circuit Data bit DI 2	Wire break /short circuit Data bit DI 1
Channel 8	Channel 7	Channel 6	Channel 5	Channel 4	Channel 3	Channel 2	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

15.1.1.8 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 234: 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	Signal status DI 7	Signal status DI 6	Signal status DI 5	Signal status DI 4	Signal status DI 3	Signal status DI 2	Signal status DI 1
Channel 8	Channel 7	Channel 6	Channel 5	Channel 4	Channel 3	Channel 2	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	Wire break /short circuit Data bit DI 7	Wire break /short circuit Data bit DI 6	Wire break /short circuit Data bit DI 5	Wire break /short circuit Data bit DI 4	Wire break /short circuit Data bit DI 3	Wire break /short circuit Data bit DI 2	Wire break /short circuit Data bit DI 1
Channel 8	Channel 7	Channel 6	Channel 5	Channel 4	Channel 3	Channel 2	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

15.1.1.9 16 Channel Digital Input Modules

750-1400, -1402, -1405, -1406, -1407

Table 235: 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

15.1.2 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.

15.1.2.1 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 236: 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

15.1.2.2 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 237: 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

15.1.2.3 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 238: 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 239: 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

15.1.2.4 4 Channel Digital Output Modules

750-504, -515, -516, -519, -531,
753-504, -516, -531, -540

Table 240: 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

15.1.2.5 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 241: 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

15.1.2.6 8 Channel Digital Output Module

750-530, -536, -1515, -1516,
753-530, -534, 536

Table 242: 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

15.1.2.7 8 Channel Digital Output Modules with Diagnostics and Input Process Data750-537,
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 243: 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

15.1.2.8 16 Channel Digital Output Modules

750-1500, -1501, -1504, -1505

Table 244: 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

15.1.2.9 8 Channel Digital Input/Output Modules

750-1502, -1506

Table 245: 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	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
Channel 8	Channel 7	Channel 6	Channel 5	Channel 4	Channel 3	Channel 2	Channel 1

Output Process Image							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
controls DO 8	controls DO 7	controls DO 6	controls DO 5	controls DO 4	controls DO 3	controls DO 2	controls DO 1
Channel 8	Channel 7	Channel 6	Channel 5	Channel 4	Channel 3	Channel 2	Channel 1

15.1.3 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.

15.1.3.1 1 Channel Analog Input Modules

750-491, (and all variations)

Table 246: 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}

15.1.3.2 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 247: 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

15.1.3.3 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 248: 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 249:: 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	-	-	

15.1.3.4 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 250: 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

15.1.3.5 8 Channel Analog Input Modules

750-451, 750-458, 750-496, 750-497

Table 251: 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

15.1.3.6 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 252: 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 253: 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	-	-	

15.1.4 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.

15.1.4.1 2 Channel Analog Output Modules

750-550, -552, -554, -556, -560, -562, 563, -585, -586, (and all variations),
753-550, -552, -554, -556

Table 254: 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

15.1.4.2 4 Channel Analog Output Modules

750-553, -555, -557, -559,
753-553, -555, -557, -559

Table 255: 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

15.1.5 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.

15.1.5.1 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 256: 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 257: 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 258: 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 259: 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

15.1.5.2 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 260: 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

15.1.5.3 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 261: 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	

15.1.5.4 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 262: 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		

15.1.5.5 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 263: 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

15.1.5.6 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 264: 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	

15.1.5.7 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 265: 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 266: 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		

15.1.5.8 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 267: 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 268: 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 269: 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 270: 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	

15.1.5.9 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 271: 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

15.1.5.10 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 272: 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)

15.1.5.11 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 273: 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		

15.1.5.12 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 274: 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	-	S	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	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
9	GA4...GA7	GA0...GA3	
10	GA12...GA15	GA8...GA11	
11	Bit 8...15	Bit 0...7	Switch scene 0...15

DA = DALI address
GA = Group address

Table 275: 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		

15.1.5.13 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 276: 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		

15.1.5.14 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 277: 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	

15.1.5.15 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 278: 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		

15.1.5.16 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 279: *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

15.1.5.17 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 280: 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)	

15.1.5.18 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 281: 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

15.1.5.19 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 data.

The mailbox and the process image sizes are set with the startup tool **WAGO-I/O-CHECK**.

Table 282: 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

15.1.6 System Modules

15.1.6.1 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 283: 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 284: 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

15.1.6.2 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 285: 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

15.1.6.3 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 286: 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

Glossary

A

ASHRAE (American Society of Heating, Refrigerating and Air-Conditioning Engineers)

ASHRAE is an American professional association for HVAC engineering that was founded in 1894.

ASHRAE prepares and publishes manuals, magazines, standards and guidelines for the air-conditioning sector.

The BACnet protocol has been the standard for ASHRAE since 1995 and was accepted by ANSI in 2004 (ANSI/ASHRAE 135-2004).

B

BACnet (Building Automation and Control Networks)

BACnet denotes a fieldbus, a protocol, a standard or a process that can be used to compatibly exchange data between devices of various manufacturers. BACnet was developed in 1987 by ASHRAE for building automation services and has become anchored in different standards since then (ASHRAE/ANSI standard (135-2004), DIN EN ISO standard (16484-5)). BACnet is primarily oriented toward the HVAC sector.

BACnet standard objects and properties, which can be accessed by likewise standardized services, are defined in the standard to achieve the required interoperability.

Manufacturers publish in a document (PICS) those BACnet standard objects, properties and services that they support. This information is provided in blocks broken down into the various functions (BIBBs). Devices are classified in five device profiles to permit easier comparison of the BACnet devices with regard to their various functions and the different possible combinations of objects and services. Each device profile specifies defined minimum requirements for the BACnet functionality that is implemented, facilitating the selection of a suitable device by the customer for specific applications.

BACnet is suitable for the field level as well as the automation level.

BACnet Configurator

The BACnet Configurator is free software that is used for commissioning and configuration of WAGO BACnet couplers/controllers. This includes, among other things, logical structuring of the project and network, addressing of the coupler/controller, configuration of the client and the service in every BACnet device and a value browser (for BACnet object properties). The BACnet Configurator is separate, dedicated software and should not be confused with the I/O Configurator for the WAGO-I/O-PRO.

BACnet Data Types

Services utilize standardized BACnet data types and communication units, so-called application layer protocol data units (APDUs) that are defined in an abstract ASN.8824 syntax in accordance with ISO Standard 1 to ensure uniform data transfer.

Elementary data types such as BOOLEAN and INTEGER, and defined BACnet base types are used which consist of SEQUENCES und CHOICES, for example. The latter are made up of elementary or nested, compiled data types.

BACnet/IP

BACnet/IP is a standardized and company-neutral network protocol for building automation services used primarily in the HVAC sector.

This protocol supports building-specific, standard objects and services for integrating devices within networks to ensure interoperability.

This protocol is defined in three (3) layers: BACnet Virtual Link Layer (BVLL) as a backup and bit transfer layer, BACnet Network Layer as the transfer layer and BACnet Application as the application layer. ARCNET, ETHERNET, BACnet/IP, PTP (Point-To-Point) are supported via RS232; MS/TP (Master Slave/Token Passing) via RS485 and LonTalk ANSI/EIA709.1 on the backup and bit transfer layer.

Communication between different devices is executed based on the client/server method, with each device able to act as a client or as a server.

This protocol, which has been an ASHRAE standard since 1995, was accepted as a standard by ANSI (ANSI/ASHRAE 135-2004) and has become anchored in the DIN EN ISO standard 16484-5 (Building Automation Systems, Data Communication Protocols).

BACstac

Function libraries that implement the BACnet protocol and interfaces with well-known high-level languages are known as BACstacs. BACstacs are generally available on the market. BACstacs simplify and accelerate the development of new BACnet devices, as protocol communication at the lowest level is already implemented by BACstac, enabling the developer to build directly upon the application level.

Baseband

Baseband systems are systems that operate without carrier frequencies, i.e. with non-modulated signals. This means they provide exactly one channel that must be logically adapted to the various, specific requirements. Opposite: Broadband

BBMD (BACnet Broadcast Management Device)

BACnet uses broadcast messages ("to everyone") for data communication via networks. Many routers block broadcasts. This is why special routers, BBMDs, are used in networks. A BBMD receives a broadcast that is to be sent to a different network and transmits it directly to the BBMD in the other network. The BBMD receiving the message then transmits the broadcast within its local network. This allows the broadcast to be received by the target device.

B-BC (BACnet-Building-Controller)

The BACnet Building Controller forms one of six different device profiles

described by the BACnet Standard. The B BC is comparable to a control system in building automation services (Direct Digital Control (DDC)).

To meet the requirements of the BACnet Standard for a B-BC, or for a defined device profile, certain BACnet objects, services, etc., must be implemented in the device. These are defined by the function blocks (BIBBs).

The BIBBs that are supported by the device are entered in a document (PICS) that serves as the basis for communication and comparison for manufacturers and customers.

BIBB (BACnet Interoperability Building Block)

A BIBB defines which BACnet features must be implemented in a device for each task. Compared to the BIBBs from different manufacturers, common features represent a basis for interoperability between the devices. BIBBs form the function blocks for the specific interoperability area (IA) and define the functions within this base.

A BIBB is formed from the IA in which it is contained, the Service that can be used and the user (client or server).

Example: DS - RP - A (consisting of IA (DS), Service (RP), User (A))

BIBBs are published in the manufacturers PICS. The Device profile is classified on the basis of the supported BIBBs.

BIG EU (BACnet Interest Group Europe)

The BIG EU is made up of famous members of the building, planning and production industries as well as different training facilities. It publishes reference solutions in the BACnet area to support planners who work in this field. Among other things the NISTIR (National Institute of Standards and Technology Interagency Report) Guideline is also published (<http://www.big-eu.de>).

Bit

Smallest information unit. Its value can either be 1 or 0.

Bit Rate

Number of bits transmitted within a time unit.

BootP

The Bootstrap Protocol sends configuration data to several controllers/computers, etc. (without hard drives). This eliminates the need for manual, individual configuration.

BootP is used at WAGO for assigning IP addresses to couplers/controllers. DHCP reverts back to BootP.

Bridge

A bridge runs on Layer 2 of the ISO/OSI model. Although the bridge corresponds to a Switch, it has only one output, however.

Bridges separate the network into Segments, allowing the number of nodes to be increased. Corrupt data is filtered out. Telegrams are then sent when the target address is located in the linked Segment. Only the frame of the MAC layer is treated. If the destination address is known, the bridge then forwards the data (when the destination address is on a different string than the one where the Frame originated), or destroys it (subscriber already has the frame). If you do not

know the address, the bridge forwards the data in all its known Segments and notes the source address.

A bridge is used to transfer messages independently of the message destination.

Broadband

Transmission technique using a high bandwidth to permit high data transfer rates. This technique allows several devices to transmit simultaneously.

Opposite: Baseband

Broadcast

Broadcast. A message that is sent to all stations connected to the network.

Bus

Bus is a general designation for a line used for bit-parallel or bit-serial data transfer. The bus consists of address, data, control and supply bus. The width of the bus (8, 16, 32, 64-bit) and its frequency are the determining factors for the data transmission rate. The width of the address bus limits network expansion. The fieldbus is a special type of serial bus.

Byte (Binary Yoked Transfer Element)

A data element larger than a bit and smaller than a word. A byte generally contains 8 bits. A byte may contain 9 bits in 36-bit computers.

C

Client

Service-requesting device within the Client Server System. With the aid of the service request, the client can access objects (data) on the Server. The service is provided by the server.

Coaxial Cable

This cable contains one, single conductor and radial shielding for transmitting information.

CSMA/CD (Carrier Sense Multiple Access/Collision Detection)

Random bus access procedure (Carrier Sense Multiple Access with Collision Detection). When a collision is detected, all subscribers back. After waiting (a random delay time), the subscribers attempt to re-transmit the data.

D

Deterministic ETHERNET

Deterministic ETHERNET denotes that the runtimes can be defined and

calculated in an ETHERNET network. This is possible by setting up a Switched ETHERNET.

Device profiles (BACnet)

Six (6) device profiles are defined, with each one classifying a minimum number of functions/BIBBs that are supported.

Classification for the devices is specified in Appendix L of the BACnet standards and can be used to determine interoperability in the specific IAs.

Standardized Device Profile:

B-OWS	BACnet Operator Workstation
B-BC	BACnet Building Controller
B-AAC	BACnet Advanced Application Controller
B-SA	BACnet Smart Actuator
B-SS	BACnet Smart Sensor
B-GW	BACnet Gateway

BACnet Gateway Device profiles are published in the manufacturer PICS and make it easier for the customer to compare different BACnet devices with respect to their functions and interoperability.

DHCP (Dynamic Host Configuration Protocol)

This protocol permits automatic configuration of the network for a computer, and also assigns addresses or sets parameters centrally. The DHCP server uses a fixed IP address pool for automatically assigning random, temporary IP addresses to networked computers (Clients) or couplers/controllers, thus saving considerable configuration work in large networks. The client also obtains other information, such as the gateway address (router) and the IP address of the Domain Name System (DNS).

DNS (Domain Name System)

The Domain Name System is a distributed, decentralized database that manages the name sector in the Internet. Unique domain names (such as <http://www.wago.de>) are transformed into IP addresses (such as 123.45.67.123) using a "forward lookup." IP addresses can be converted back to domain names using a "reverse lookup." Using the naming service several IP address can be used for one domain name for distribution of network load. Besides this, domain names are easier to remember than IP addresses. If an IP address changes in the background, this does not affect the domain name. Paul Mockapetris developed the DNS in 1983. Since then it has been expanded to include other standards and has become anchored in the RFC 1034 and RFC.

Driver

Software code, which communicates with a hardware device. This communication is normally performed by internal device registers.

E

EDE (Electronic Data Exchange)

The EDE file serves as a configuration aid for coordinating the functions between devices from different suppliers or commissioning parties. . This file contains the addresses set in the BACnet Configurator and the names of the devices and objects, along with the values for the object properties. Generation of the EDE file for the WAGO BACnet coupler/controller can be started directly from the user interface for the BACnet Configurator.

In the "Server" mode the objects for the BACnet coupler/controller can be exported into an EDE file. In the "Client" mode, external objects can be imported using the EDE file.

EIB (European Installation Bus)

see KNX

ETHERNET

Specifies a Local Area Network (LAN), which was developed by Xerox, Intel and DEC in the 70's. The bus access process takes place according to the CSMA/CD method.

ETHERNET Standard

ETHERNET was standardized in 1983 with IEEE 802.3 10Base5. ISO accepted this standardization with the ISO Standard 8802/3. ETHERNET can, in the meantime, be used with all common types of cables and with optic fibers. There are, however, some technical and considerable logical differences between the standardized variants and the original "ETHERNET," which is why the term "ETHERNET" is used when the older design is meant and "802.3" is used for standardized systems. The essential differences between the ETHERNET and the IEEE standard are found in the frame architecture and in the handling of pad characters.

F

Fieldbus

The fieldbus is a dedicated bus for the serial transmission of information. Fieldbus systems connect sensors, actuators and controls from the field level to the management level. Numerous different fieldbus systems have been developed for various purposes. For example, the BACnet, LON and KNX fieldbus systems are used primarily in building automation, whereas CANbus and Interbus are applied chiefly in the automotive industry.

Firewall

Collective name for solutions that protect LANs from unauthorized access from the internet. They are also able to control and regulate the traffic from the LAN

into the Internet. The crucial part of firewalls is static Routers, which have an access control list used to decide which data packets can pass from which Host.

Frame

Unit of data transferred at the Data-Link layer. It contains the header and addressing information.

FTP (File Transfer Protocol)

A standard application for TCP/IP, which permits files to be transferred without files being accessed.

Function

Functions are modules that always return the same results (as a function value) when the input values are identical. They have no local variables that store values beyond an invoke.

Function Block

Function blocks are used for IEC 61131 programming and stored in libraries for repeated utilization. A function block is a structured module, which has a name and contains input and output variables, as well as local variables.

G

Gateway

Device for connecting two different networks, performs the translation between differing protocols.

H

Hardware

Electronic, electric and mechanical components of a module.

Header

A portion of the data packet, containing information such as the receiver's address information.

Host

Originally used to describe a central mainframe computer accessed from other systems. The services provided by the subscriber can be called up by means of local and remote request. Today, host can also refer to computers that provide certain services from a central location (such as UNIX hosts on the Internet).

HTML (Hypertext Markup Language)

HTML is the descriptive language for documents on the World Wide Web. It contains language elements for the design of hypertext documents.

HTTP (Hyper Text Transfer Protocol)

Client/Server TCP/IP protocol, which is used on the Internet or Intranets for exchange of HTML documents. It normally uses Port 80.

Hub

A device, which allows communication between several network users via twisted pair cable. Its topology is star-shaped.

HVAC (Heating, Ventilation and Air Conditioning)

HVAC is a special sector of building automation services.

Hypertext

Document format used by HTTP. Hypertext documents are text files that provide links to other text documents via particular highlighted keywords.

I**ICMP (Internet Control Message Protocol)**

ICMP is a protocol for transmission of status information and error messages of the IP, TCP and UDP protocols between IP network nodes. ICMP offers, among other things, the possibility of an echo (ping) request to determine whether a destination is available and is responding.

IEC 61131-3

International standard for modern systems with PLC functionality created in 1993. Based on a structured software model, it defines a series of powerful programming languages to be utilized for different automation tasks. AWL (statement list - STL), ST (structured text), AS (process structure), FUP (function plan), KOP (contact plan).

IEEE

Institute of Electrical and Electronic Engineers.

IEEE 802.3

IEEE 802.3 is an IEEE standard. ETHERNET only supports the yellow cable as a medium (Thicknet ETHERNET coaxial cable). IEEE 802.3 also supports S UTP and Broadband coaxial cable. The segment lengths range from 500 m for yellow cable, 100 m for TP and 1800 m for Broadband coaxial cable. A star or bus topology is possible. ETHERNET (IEEE 802.3) uses CSMA/CD as a channel access method.

Intel Format

Set configuration for the coupler/controller for setting up the process image. In the coupler/controller memory, the module data is aligned in different ways,

depending on the set configuration (Intel/Motorola-Format, word alignment, etc.). The format determines whether or not high and low bytes are changed over – they are not changed with the Intel format.

Internet

A collection of networks interconnected to each other throughout the world. It is most commonly referred to as the World Wide Web, or simply as the Web.

Interoperability

Interoperability is the capability of different devices, systems, methods or even organizations to find a common language for mutually achieving a set goal. Systems and software operate with interoperability, for example, when they are linked via interfaces, when they use common network protocols and data formats, or when they contain the same standards. These conditions enable information and data to be exchanged and provided in an efficient manner.

Interoperability Area (IA)

To evaluate the overall interoperability of a system the requirements made on the individual devices are broken down into seven areas (Interoperability Areas) according to their functions. These then serve as the basis for evaluating the interoperability.

The following IAs are defined: Data Sharing (DS), Alarm and Event Notification (AE), Scheduling, (SCHED), Trending (T), Device Management (DM), Network Management, Network Management (NM) und Virtual Terminal Management (VT).

Each of these IAs possesses a collection of interoperability or function modules, the BIBBS. These modules define all services that a client or server can perform with the IA.

The abbreviation for the IA (e.g. DS) is placed in front of the BIBB name.

Intranet

A private network within an organization that allows users to exchange data within that particular organization.

I/O Configurator

The I/O Configurator is a plug-in incorporated into WAGO-I/O-PRO for easier assignment of addresses and protocols for modules at a coupler/controller.

IP (Internet Protocol)

Internet protocol is a network protocol that performs packet-oriented, connectionless and non-acknowledged transfer of data within a network. This protocol builds upon the transfer layer for the ISO/OSI model. Stations identify themselves using IP addresses.

IP Message Tunneling

In addition to BACnet/IP, IP message tunneling is a method for transferring BACnet messages to a network.

Communication via IP message tunneling takes place via the BACnet tunneling router (BTR), which is also designated as “Annex H Router” on account of its description in the annex of the BACnet Standard.

Implementation between the different communication technologies BACnet and

IP is performed using routing tables, with a combination of BACnet network numbers and IP addresses. The BACnet protocol requires an Annex H router in both local area networks in order to send a message from one device to another one on a different network. The Annex H router for the first network transfers the BACnet message to a UDP (User Datagram Protocol) frame and transmits the message over standard IP links, or over the Internet to the Annex H router in network 2.

This router then “unpacks” the incoming data packet and sends the message to the destination device via the BACnet protocol.

BACnet devices do not require IP compatibility for IP message tunneling via BTRs. BTRs are frequently used in existing BACnet networks that have a link to IP networks, to an intranet or to the Internet.

ISO/OSI (Open Systems Interconnection) Model

The ISO/OSI model is a reference model for networks, with the goal of creating open communication. It defines the interface standards of the respective software and hardware requirements between computer manufacturers. The model treats communication removed from specific implementations, using seven layers. The model treats communication removed from specific implementations, using seven layers: 1 -Bit transfer layer, 2 -Backup layer, 3 -Transfer layer, 4 -Transport layer, 5 -Session layer, 6 -Presentation layer and 7 -Application layer.

K

KNX

KNX has been established as a flexible bus system for building automation and has been standardized by the KNX Association in ISO/IEC 14543. KNX was developed by the European installation bus (EIB), BatiBUS and European Home Systems (EHS). In addition to twisted pair, other transmission media, such as powerline, radio and links to ETHERNET (“KNXnet/IP”) are also supported.

L

LAN (Local Area Network)

A LAN is a spatially limited, local network for permanently linking computers over shorter distances. Data transfer can take place via ETHERNET, Token Ring and FDDI, as well as wireless (WLAN).

Library

Collection of Modules available to the programmer in the WAGO-I/O-PRO programming tool for creating control programs in accordance with IEC61131-3.

LON (Local Operating Network)

LON is used as a fieldbus for building automation. It was developed 1990 by

Echelon and enables, as does KNX, the communication between different devices, independent of the manufacturer and active application.

M

MIB (Management Information Base)

MIB is a collection of information about all parameters, which can be handed over to the management software with a request via SNMP. This enables remote maintenance, monitoring and control of networks to be performed via SNMP protocol.

MODBUS

MODBUS is an open protocol based on the Master/Slave principle. The MODBUS links the master with several clients, via either serial interface or ETHERNET.

Three data transmission types are available: MODBUS/RTU (binary data transmission), MODBUS/TCP (data transmission using TCP/IP packets) and MODBUS/ASCII (ASCII code transmission).

Module

Modules consist of functions, function blocks and programs.

Every module is made up of a declaration part and a body. The body is written in one of the IEC programming languages AWL (statement list - STL), ST (structured text), AS (process structure), FUP (function plan) or KOP (contact plan).

O

Object

BACnet communication takes place using standardized objects (DIN EN 16484-5). These objects are tailored specifically to the HVAC sector for building automation services. Both simple field devices as well as complex automation control systems can be modeled in the object presentation. Objects may represent both physical inputs and outputs and virtual objects, such as counting values.

Objects possess certain properties, whose values can be read and/or written using services.

All of the objects supported by a device are also described in the PICS data from the specific manufacturer.

Open MODBUS/TCP Specification

Specification, which establishes the specific structure of a MODBUS/TCP data packet. This is dependent upon the selected function code or upon the selected function (import or export bit or register).

Operating System

An operating system is software used for managing equipment such as memory and connected devices, and for executing programs.

P**Parameter Setting**

Parameterization is defined as the assignment and storage of set-up and configuration data as they are required for the execution of predefined functions.

Ping Command

When a ping command (ping < IP address) is entered, the ping program ICMP generates echo request packets. It is used to test for node availability.

Port Number

The port number, in conjunction with the IP address, is the unique connection point between two processes (applications).

Predictable ETHERNET

The predictable message delay time on an ETHERNET network. The measures that are taken here enable nearly real-time requests to be realized.

Prioritization

BACnet applications can access Objects through Services and change their properties. Access prioritization is required to regulate and organize access of various applications to the properties. The BACnet standard distinguishes between 16 different priority levels. A priority can only be set for the current values (Present_Value) of output objects. For this reason they are also called "command properties". The processing sequences for individual applications can be changed using prioritization. Simultaneous access of several applications to the same Objects is regulated in this manner. The application with the highest priority level (lowest number) is given priority.

Property

Objects are described by specific properties and values. In this manner, object information, such as name, status and behavior of an object can be read.

Properties may be editable and readable (R), readable and writable (W) and optionally readable and/or writable (O). Access to object properties is gained using Services.

The properties Object_Identifier, Object_Name, Object_Type and Present_Value are common to all Objects. Other properties are object-specific, depending on the function.

Protocol Implementation Conformance Statement (PICS)

The Protocol Implementation Conformance Statement (PICS) described objects and functions supported by BACnet devices. This is a standard document that must be filled in by the manufacturer. When linking different systems, the PICS and the BIBBs for the devices contained therein are compared with one another.

Proxy Server

Proxy means agent or representative. A proxy server (or proxy gateway) allows indirect access to the network by systems, which do not have direct access to the Internet. This may be systems that are restricted from direct access by a firewall

for security reasons. A proxy can filter out individual data packets between the Internet and a local network LAN to enhance security. Proxies are also used to limit access to particular servers.

In addition, proxy servers can also have a cache function. In this case they check whether the respective URL address is already available locally and return it immediately, if necessary. This saves time and costs associated with multiple accesses. If the URL is not in the cache, the proxy forwards the request as normal.

The user should not notice the proxy server apart from the single configuration in the web browser. Most web browsers can be configured so that they use different or no proxy gateways per access method (FTP, HTTP).

R

Repeater

Repeaters operate (like hubs, but with only one, instead of several outputs) on Layer 1 of the ISO/OSI model.

Repeaters are physical amplifiers without their own processing function. They refresh data without detecting damaged data and forward all signals. Repeaters are used for implementing greater transmission distances, or when the maximum number of nodes of (normally) 64 devices for each twisted-pair segment is exceeded. The repeater is then always counted as a node in a segment when the maximum number of nodes is reached.

The media can also be changed when routers are used that are configured as repeaters.

Request

A service request from a client, which requests the provision of a service from a server.

Response

Response from a server in reply to a request from a client.

RFC Specifications

Specifications, suggestions, ideas and guidelines regarding the Internet are published in the form of RFCs (Request For Comments).

RJ-45 Connector

The RJ-45 plug is also referred to as a Western connector. This connector creates the connection of two network controllers via a twisted-pair cable.

Router

Routers are used to connect neighboring subnets, with the router operating with addresses and protocols of the third ISO/OSI layer. As this layer is hardware independent, the routers allow transition to another transmission medium.

To transmit a message the router evaluates the logical address (source and

destination address) and finds the best path if there are several possibilities. Routers can be operated in the Repeater or Bridge modes.

Routing

Method of selecting the best path for sending data to a distant network.

RS-232

The RS-232 (official designation ANSI/EIA/TIA-232-F-1997) is a serial interface for point-to-point connections. "RS" stands for "Radio Sector", but is frequently translated as "Recommended Standard".

Data is transmitted via this interface bit-serial over a data line and received on a different data line. As only one data line is used at a time, the data is transmitted time-delayed consecutively and asynchronously. The time intervals between transmissions of the data may be randomly long.

As the RS-232 interface is a so-called powered interface, data is transferred electrically encoded.

The cable connections used for this interface are 9-pin Sub-D connectors and 9-pin jacks. A distinction is made here between data lines (RxD, TxD and GND) and control lines (DCD, DTR, DSR, RTS, CTS and RI).

S

SCADA (Supervisory Control and Data Acquisition)

SCADA software is a program for the control and visualization of processes (supervisory control and data acquisition).

Segment

Typically, a network is divided up into different physical network segments by way of routers or repeaters.

Server

Service-supplying device within a Client Server System. The service is requested by the Client.

Service

A service is an operation (Read, Write) oriented toward an object.

BACnet specified standardized services that are transmitted via a special BACnet network layer. Communication is based on the client/server method: The client makes requests to the server. The server processes the requests from the client and then transmits a response. A distinction is made between 38 services that are broken down into 5 categories: Alarm and events, object access, file access, remote device access, and virtual terminal services

Service port

The service port is located next to the mode switch, behind the cover flap on the controller. This port acts as the configuration and programming interface and is

used for communication with WAGO-I/O-*CHECK*, WAGO-I/O-*PRO* and for downloading firmware. A special programming cable (750-920) is necessary.

SMTP (Simple Mail Transfer Protocol)

Standard protocol, with which E-mails are sent via Internet.

SNMP (Simple Network Management Protocol)

SNMP is used for remote maintenance of servers. This allows routers, for example, to be configured directly from the network provider's office, without having to physically visit the customer.

SNTP (Simple Network Time Protocol)

This connectionless network protocol performs time synchronization in networks with a time server via Internet. SNTP is a simplified version of the NTP protocol. On account of this simplification (also with regard to the software), SNTP operates somewhat less exact than NTP. SNTP is defined in RFC 4330.

Socket

A software interface implemented with BSD-UNIX for inter-process communication. Sockets are also possible in the network via TCP/IP. Per Windows 3.11, they are also available in Microsoft operating systems.

STP (Shielded Twisted Pair)

An STP cable is a symmetrical cable with shielded cores twisted in pairs. The classic STP cable is a multi-core cable, whose stranded conductors are isolated. The conductors of the STP cable are individually protected; it has no total shielding.

S-STP (Screened/Shielded Twisted Pair)

In addition to STP cables, S-STP cables are provided with total shielding consisting of foil or network shielding in addition to the single shielding for the individual conductors.

Structured Cabling

With structured cabling, maximum permissible cable lengths are defined (EIA/TIA 568, IS 11801) for site, building and floor cabling, with recommendations for topologies also indicated.

Subnet

A portion of a network that shares the same network address as the other portions. These subnets are distinguished through the subnet mask.

Subnet Mask

Subnet masks can be used to manipulate the address ranges in the IP address area in reference to the number of subnets and hosts. A standard subnet mask, for example, is 255.255.255.0.

S/UTP (Screened Unshielded Twisted-Pair)

Screened twisted pair cable, which only has one external shield. However, the twisted pair cables are not shielded from each other.

Switch

Switches are comparable to bridges, but with several outputs. Each output uses the full ETHERNET bandwidth. Each output uses the full ETHERNET bandwidth. Switches learn which nodes are connected and filter the information transmitted over the network accordingly. Switches learn which nodes are connected and filter the information transmitted over the network accordingly.

Switched ETHERNET

ETHERNET network set up using switches. There are a multitude of applications for switching technologies. ETHERNET switching is becoming increasingly popular in local networks as it allows deterministic ETHERNET.

T**TCP (Transport Control Protocol)**

TCP is a connection-oriented network protocol for the transport layer (Layer 4) of the ISO/OSI model provided with relatively secure transmission mechanisms.

TCP/IP Protocol Stack

The TCP/IP protocol stack denotes network protocols that enable communication between different networks and topologies.

Telnet

The Telnet protocol fulfils the function of a virtual terminal. It allows remote access from the user's computer to other computer systems on the network.

Traps

Traps are unsolicited messages, which are sent by an "agent" to a management system, as soon as something unexpected and interesting for the management system happens. Traps are comparable to interrupts from hardware. A well-known example of a trap message is the "Blue screen" with Win95/98.

Twisted Pair

Twisted pair cables (abbreviated to TP).

U

UDP (Users Datagram Protocol)

The user datagram protocol is a communication protocol between two computers and an alternative to TCP (Transmission Control Protocol). As with TCP, UDP communicates via Internet Protocol, although it is somewhat less reliable due to its uncontrolled communication method.

URL (Uniform Resource Locator)

Address form for Internet files which are mostly applied within the World Wide Web (WWW). The URL format makes a unique designation of all documents on the internet possible. It describes the address of a document or objects that can be read by a web browser. URL includes the transmission type (HTTP, FTP), the computer that contains the information and the path on the computer. A URL has the following format:

Document type://Computer name/List of contents/File name.

UTP (Unshielded Twisted Pair)

The UTP cable is a symmetrical, non-protected cable with twisted colored wires in pairs. This cable type, either of a two-pair or four-pair design, is the cable type most used for floor wiring and terminal wiring.

V

Vendor ID (BACnet)

The BACnet standard defines numerical identifiers for suppliers. These IDs can be obtained free of charge from ASHRAE and are a prerequisite for development, marketing and operation of BACnet components in a standard BACnet network.

The vendor ID for WAGO Kontakttechnik GmbH & Co. KG is "222". A list of all assigned vendor IDs is available at the following Internet page:

<http://www.bacnet.org/VendorID/index.html>

W**WAGO-I/O-PRO (CODESYS)**

Uniform programming environment, programming tool by WAGO Kontakttechnik GmbH & Co. KG for the generation of a control program as per IEC61131-3 for all programmable fieldbus controllers (PFC). The software enables an application program to be created, tested, debugged and started up.

WAGO-I/O-PRO consists of the basic tool "CODESYS 2.3" and the target files with the WAGO-specific Drivers.

Web Browser

A Web browser is a program used for reading Hypertext. The browser allows the various documents to be viewed in Hypertext and navigation between documents.

Word Alignment

Set configuration for the fieldbus coupler/controller for setting up the process image. Word-alignment is used to establish the process image word-by-word (2 bytes).

WWW (World Wide Web)

The World Wide Web (network) is a Hypertext system that can be called up via Internet. It is based on the HTTP network protocol, the descriptive language HTML and URLs for unique page (site) addressing.

Literature List



Information

Switching Technology in the Local Network

Mathias Hein
Thomson Executive Press
ISBN 9781850321668

TCP/IP 2: Running a Successful Network

(Data Communications and Networks Series)
Kevin Washburn, Jim Evans
Addison-Wesley Publishing Company, 1996
ISBN 9780201877113

Local Area Networks - An Introduction to the Technology

John E. McNamara
Digital Press, 1995
ISBN 9780135330500

Information on the Internet:

Fit in one day for TCP/IP sockets

Last updated Aug. 2019

Wiesemann & Theis GmbH
<http://www.wut.de>

BIG EU (BACnet Interest Group Europe)

Last updated Aug. 2019

The BIG-EU publishes reference solutions in the BACnet area to support planners who work in this field. Among other things the NISTIR (National Institute of Standards and Technology Interagency Report) Guideline is also published.
<http://www.big-eu.de/eng>

ASHRAE (American Society of Heating, Refrigeration and Air-Conditioning Engineers)

Last updated Aug. 2019

Professional association for all employed in the heating, cooling, ventilation and air-conditioning fields in the USA
<http://www.ashrae.org>

ASHRAE SSPC 135 Committee

Last updated Aug. 2019

The "Standing Standard Project Committee 135" steers the ongoing development of the protocol
<http://www.bacnet.org>

List of Figures

Figure 1: View	29
Figure 2: Marking Area for Serial Numbers	32
Figure 3: Update Matrix from 2016	33
Figure 4: Data Contacts	34
Figure 5: Power Jumper Contacts	35
Figure 6: CAGE CLAMP® connections	36
Figure 7: Service Interface (Closed and Open Flap)	37
Figure 8: Network Connections – X1, X2	38
Figure 9: RS-232/RS-485 – Communication Connection – X3	39
Figure 10: Termination with DTE-DCE Connection (1:1)	40
Figure 11: Termination with DCE-DCE Connection (Cross-Over)	40
Figure 12: RS-485 Bus Termination	41
Figure 13: Power Supply Indicating Elements	42
Figure 14: Indicating Elements for System/Fieldbus	43
Figure 15: Indicating Elements, Memory Card Slot	44
Figure 16: Indicating Elements, RJ-45 Jacks	45
Figure 17: Mode Selector Switch	46
Figure 18: Reset Button	47
Figure 19: Slot for SD Memory Card	48
Figure 20: Schematic diagram	49
Figure 21: Connecting the Controller to a Cloud Service (Example)	83
Figure 22: Spacing	97
Figure 23: Release Tab of Controller	99
Figure 24: Connecting a Conductor to a CAGE CLAMP®	100
Figure 25: Power Supply Concept	102
Figure 26: “Open DHCP”, Example Figure	106
Figure 27: “WAGO Ethernet Settings” – Starting Screen (Example)	107
Figure 28: “WAGO Ethernet Settings” – “Network” Tab	108
Figure 29: Example of a Function Test	110
Figure 30: Entering Authentication	116
Figure 31: Password Reminder	117
Figure 32: WBM Browser Window (Example)	119
Figure 33: WBM Status Information (Example)	120
Figure 34: CBM main menu (example)	192
Figure 35: “WAGO Ethernet Settings” – Start Screen	240
Figure 36: “WAGO Ethernet Settings” – Communication Link	241
Figure 37: “WAGO Ethernet Settings” – Identification Tab (Example)	242
Figure 38: “WAGO Ethernet Settings” – Network Tab	243
Figure 39: “WAGO Ethernet Settings” – Protocol Tab	245
Figure 40: “WAGO Ethernet Settings” – Status Tab	246
Figure 41: Remanent Main Memory	249
Figure 42: Modbus Address Overview	250
Figure 43: State Diagram, ADVANCED_WATCHDOG Operation Mode	253
Figure 44: State Diagram, SIMPLE_WATCHDOG Operation Mode	254
Figure 45: State Diagram, Switching Operation Modes	254
Figure 46: Power Supply Indicating Elements	262
Figure 47: Indicating Elements for System/Fieldbus	263

Figure 48: Indicating Elements, RJ-45 Jacks	268
Figure 49: Flashing Sequence Process Diagram	270
Figure 50: Inserting the Memory Card	279
Figure 51: Release Tab of Controller.....	285
Figure 52: Marking Example According to ATEX and IECEx	289
Figure 53: Text Detail – Marking Example According to ATEX and IECEx	289
Figure 54: Marking Example for Approved Ex i I/O Module According to ATEX and IECEx	291
Figure 55: Text Detail – Marking Example for Approved Ex i I/O Module According to ATEX and IECEx	291
Figure 56: Marking Example According to NEC	293
Figure 57: Text Detail – Marking Example According to NEC 500	293
Figure 58: Text Detail – Marking Example for Approved Ex i I/O Module According to NEC 505	294
Figure 59: Text Detail – Marking Example for Approved Ex i I/O Module According to NEC 506	294
Figure 60: Text Detail – Marking Example for Approved Ex i I/O Modules According to CEC 18 attachment J	295

List of Tables

Table 1: Number Notation.....	17
Table 2: Font Conventions.....	17
Table 3: Legend for Figure “View”	29
Table 4: Labeling Symbols	31
Table 5: Legend for Figure “Update Matrix from 2016”	33
Table 6: Legend for Figure “Power Jumper Contacts”	35
Table 7: Legend for figure “CAGE CLAMP® connections”	36
Table 8: Service Interface.....	37
Table 9: Legend for Figure “Network Connections – X1, X2”	38
Table 10: Legend for Figure “RS-232/RS-485 – Communication Connection – X3”	39
Table 11: Function of RS-232 Signals for DTE/DCE	40
Table 12: Legend for Figure “Power Supply Indicating Elements”	42
Table 13: Legend for Figure “Fieldbus/System Indicating Elements”	43
Table 14: Legend for Figure “Indicating Elements, Memory Card Slot”	44
Table 15: Legend for Figure “Indicating Elements, RJ-45 Jacks”	45
Table 16: Mode Selector Switch	46
Table 17: Technical Data – Mechanical Data	50
Table 18: Technical Data – System Data	50
Table 19: Technical Data – Power Supply.....	50
Table 20: Technical Data – Clock.....	51
Table 21: Technical Data – Programming	51
Table 22: Technical Data – Local Bus	51
Table 23: Technical Data – ETHERNET	52
Table 24: Technical Data – BACnet/IP	52
Table 25: Technical Data – Communication Interface.....	53
Table 26: Technical Data – Field Wiring.....	53
Table 27: Technical Data – Power Jumper Contacts	53
Table 28: Technical Data – Data Contacts	53
Table 29: Technical Data – Climatic Environmental Conditions	54
Table 30: Technical Data – Software Compatibility	54
Table 31: BACnet Approvals	57
Table 32: BIBBs of the B-BC	60
Table 33: WBM Users.....	73
Table 34: Linux® Users	73
Table 35: List of Parameters Transmitted via DHCP	81
Table 36: Components of the Cloud Connectivity Software Package	84
Table 37: Loading a Boot Project	93
Table 38: WAGO DIN Rails	97
Table 39: Filter Modules for 24 V Supply.....	102
Table 40: Default IP Addresses for ETHERNET Interfaces.....	105
Table 41: Network Mask 255.255.255.0	105
Table 42: User Settings in the Default State.....	117
Table 43: Access Rights for WBM Pages.....	117
Table 44: WBM “Status Information” Page – “Controller Details” Group	121
Table 45: WBM “Status Information Page – “Network Details Xn” Group(s)	122
Table 46: WBM “PLC Runtime Information” Page – “PLC Runtime” Group	123

Table 47: WBM "General PLC Runtime Configuration" Page – "General PLC Runtime Configuration" Group.....	124
Table 48: WBM "PLC WebVisu" Page – "Webserver Configuration" Group.....	125
Table 49: WBM "Configuration of Host and Domain Name" Page – "Hostname" Group.....	126
Table 50: WBM "Configuration of Host and Domain Name" Page – "Domain Name" Group.....	127
Table 51: WBM "TCP/IP Configuration" Page – "IP Configuration (Xn)" Group(s).....	128
Table 52: WBM "TCP/IP Configuration" Page – "Default Gateway n" Group	129
Table 53: WBM "TCP/IP Configuration" Page – "DNS Server" Group.....	130
Table 54: WBM "Ethernet Configuration" Page – "Switch Configuration" Group.....	131
Table 55: WBM "Ethernet Configuration" Page – "Interface Xn" Groups.....	132
Table 56: WBM "Routing" Page – "General Routing Configuration" Group.....	133
Table 57: WBM "Routing" Page – "Static Routes" Group.....	134
Table 58: WBM "Routing" Page – "IP-Masquerading" Group.....	135
Table 59: WBM "Routing" Page – "Port Forwarding" Group.....	136
Table 60: WBM "General Firewall Configuration" Page – "Global Firewall Parameters" Group.....	137
Table 61: WBM "General Firewall Configuration" Page – "Firewall Parameter Interface xxx" Group.....	138
Table 62: WBM "Configuration of MAC Address Filter" Page – "Global MAC Address Filter State" Group.....	139
Table 63: WBM "Configuration of MAC Address Filter" Page – "MAC Address Filter State Xn" Group.....	140
Table 64: WBM "Configuration of MAC Address Filter" Page – "MAC Address Filter Whitelist" Group.....	140
Table 65: WBM "Configuration of User Filter" Page – "User Filter" Group.....	141
Table 66: WBM "Configuration of User Filter" Page – "User Filter n" Group.....	141
Table 67: WBM "Configuration of User Filter" Page – "Add New User Filter" Group.....	142
Table 68: WBM "Configuration of Time and Date" Page – "Date on Device" Group.....	143
Table 69: WBM "Configuration of Time and Date" Page – "Time on Device" Group.....	143
Table 70: WBM "Configuration of Time and Date" Page – "Time Zone" Group.....	144
Table 71: WBM "Configuration of Time and Date" Page – "TZ String" Group ...	145
Table 72: WBM "Configuration of the users for the Web-based Management" Page – "Change Password for Selected User" Group.....	146
Table 73: WBM "Create Bootable Image" page – "Create bootable image from active partition" Group.....	147
Table 74: WBM "Configuration of Serial Interface RS232" Page – "Assign Owner of Serial Interface" Group.....	149
Table 75: WBM "Configuration of Serial Interface RS-232" page – "Assign Owner of Service Interface" Group.....	150
Table 76: "Firmware-Backup" WBM Page.....	152
Table 77: "Firmware Restore" WBM Page.....	154
Table 78: WBM "Mass Storage" Page – "<Device Name>" Group.....	157

Table 79: WBM “Mass Storage” Page – “<Device Name> - create new filesystem” Group.....	157
Table 80: WBM “Software Uploads” Page – “Upload New Software” Group.....	158
Table 81: WBM “Software Uploads” Page – “Activate New Software” Group ...	158
Table 82: WBM “Configuration of Network Services” Page – “Telnet” Group....	159
Table 83: WBM “Configuration of Network Services” Page – “FTP” Group.....	159
Table 84: WBM “Configuration of Network Services” Page – “FTPS” Group	159
Table 85: WBM “Configuration of Network Services” Page – “HTTP” Group	160
Table 86: WBM “Configuration of Network Services” Page – “HTTPS” Group..	160
Table 87: WBM “Configuration of Network Services” Page – “I/O-CHECK” Group	160
Table 88: WBM “Configuration of Network Services” Page – “OPC UA” Group	161
Table 89: WBM “Configuration of NTP Client” Page – “NTP Client Configuration” Group.....	162
Table 90: WBM “Configuration of PLC Runtime Services” Page – “General Configuration” Group	163
Table 91: WBM “Configuration of CODESYS Services” Page – “e!RUNTIME Webserver” Group	163
Table 92: WBM “SSH Server Settings” Page – “SSH Server” Group	164
Table 93: WBM “TFTP Server” Page – “TFTP Server” Group	165
Table 94: WBM “DHCP Configuration” – “DHCP Configuration Xn” Group	166
Table 95: WBM “Configuration of DNS Service” Page – “DNS Service” Group	167
Table 96: WBM “Modbus Services Configuration” Page – “Modbus TCP” Group	168
Table 97: WBM “Modbus Configuration Services” Page – “Modbus UDP” Group	168
Table 98: WBM “Configuration of Cloud Connectivity” Page – “Software Version” Group.....	169
Table 99: WBM “Configuration of Cloud Connectivity” Page – “Status” Group .	169
Table 100: WBM “Configuration of Cloud Connectivity” Page – “Settings” Group	170
Table 101: Dependencies of the Selection and Input Fields for the Selected Cloud Platform.....	173
Table 102: WBM “Configuration of General SNMP Parameters” Page – “General SNMP Configuration” Group.....	175
Table 103: WBM “Configuration of SNMP v1/v2c Parameters” Page – “SNMP v1/v2c Manager Configuration” Group	176
Table 104: WBM “Configuration of SNMP v1/v2c Parameters” Page – “Actually Configured Trap Receivers” Group	176
Table 105: WBM “Configuration of SNMP v1/v2c Parameters” Page – “Trap Receiver n” Group(s).....	177
Table 106: WBM “Configuration of SNMP v1/v2c Parameters” Page – “Add New Trap Receiver” Group.....	177
Table 107: WBM “Configuration of SNMP v3” Page – “Actually Configured v3 Users” Group	178
Table 108: WBM “Configuration of SNMP v3 Users” Page – “v3 User n” Group(s)	178
Table 109: WBM “Configuration of SNMP v3 Users” Page – “Add New v3 User” Group.....	179
Table 110: WBM “Diagnostic Information” Page	180

Table 111: WBM "Configuration of General BACnet" Page" – "BACnet Status" Group.....	181
Table 112: WBM "Configuration of General BACnet" Page" – "BACnet General Parameter" Group	181
Table 113: WBM "Configuration of General BACnet" Page" – "BACnet Upload" Group.....	181
Table 114: WBM "Configuration of BACnet Storage Location parameters" page – "BACnet Persistence" Group	182
Table 115: WBM "Configuration of BACnet Storage Location parameters" page – "BACnet Trendlog" Group.....	183
Table 116: WBM "Configuration of BACnet Storage Location parameters" page – "BACnet Eventlog" Group.....	183
Table 117: WBM "BACnet Diagnostic Information" page.....	184
Table 118: WBM "Configuration of OpenVPN and IPsec" Page – "OpenVPN" Group.....	185
Table 119: WBM "Configuration of OpenVPN and IPsec" Page – "IPsec" Group	185
Table 120: WBM "Configuration of OpenVPN and IPsec" Page – "Certificate Upload" Group	186
Table 121: WBM "Configuration of OpenVPN and IPsec" Page – "Certificate List" Group.....	186
Table 122: WBM "Configuration of OpenVPN and IPsec" Page – "Private Key List" Group.....	186
Table 123: "Security Settings" WBM Page – "Transport Layer Security Settings" Group.....	187
Table 124: "Advanced Intrusion Detection Environment (AIDE) WBM page" – "Run AIDE check at startup" Group.....	188
Table 125: "Advanced Intrusion Detection Environment (AIDE)" WBM page – "Control AIDE and show log" Group	188
Table 126: CBM Menu Structure	193
Table 127: "Information" Menu	195
Table 128: "Information" > "Controller Details" Submenu	195
Table 129: "Information" > "Network Details" Submenu	196
Table 130: "PLC Runtime" Menu	197
Table 131: "PLC Runtime" > "Information" Submenu	197
Table 132: "PLC Runtime" > "Information" > "Runtime Version" Submenu	197
Table 133: "PLC Runtime" > "General Configuration" Submenu	198
Table 134: "PLC Runtime" > "General Configuration" > "PLC Runtime Version" Submenu	198
Table 135: "PLC Runtime" > "General Configuration" > "Home Dir On SD Card" Submenu	199
Table 136: "PLC Runtime" > "WebVisu" Submenu.....	200
Table 137: "Networking" Menu	201
Table 138: "Networking" > "Host/Domain Name" Submenu	201
Table 139: "Networking" > "Hostname" Submenu	202
Table 140: "Networking" > "Host/Domain Name" > "Domain Name" Submenu.....	202
Table 141: "Networking" > "TCP/IP" Submenu	202
Table 142: "Networking" > "IP Address" Submenu	203
Table 143: "Networking" > "TCP/IP" > "IP Address" Submenu > "Xn"	203
Table 144: "Networking" > "TCP/IP" > "Default Gateway" Submenu	204

Table 145: "Networking" > "TCP/IP" > "Default Gateway" > "Default Gateway n" Submenu	204
Table 146: "Networking" > "TCP/IP" > "DNS Server" Submenu	205
Table 147: "Networking" > "Ethernet" Submenu	205
Table 148: "Networking" > "Ethernet" > "Switch Configuration" Submenu.....	206
Table 149: "Networking" > "Ethernet" > "Ethernet Ports" Submenu.....	206
Table 150: "Networking" > "Ethernet" > "Ethernet Ports" > "Interface Xn" Submenu	207
Table 151: "Firewall" Menu	208
Table 152: "Firewall" > "General Configuration" Submenu	209
Table 153: "Firewall" > "General Configuration" > "Interface xxx" Submenu	210
Table 154: "Firewall" > "MAC Address Filter" Submenu	212
Table 155: "Firewall" > "MAC Address Filter" > "MAC address filter whitelist" Submenu	213
Table 156: "Firewall" > "MAC Address Filter" > "MAC address filter whitelist" > "Add new / No (n)" Submenu	213
Table 157: "Firewall" > "User Filter" Submenu.....	214
Table 158: "Firewall" > "User Filter" > "Add New / No (n)" Submenu.....	215
Table 159: "Clock" Menu	216
Table 160: "Administration" Menu	217
Table 161: "Administration" > "Users" Submenu	218
Table 162: "Administration" > "Create Image" Submenu	218
Table 163: "Package Server" Menu	219
Table 164: "Package Server" > "Firmware Backup" Menu	219
Table 165: "Package Server" > "Firmware Backup" > "Auto Update Feature" Menu.....	220
Table 166: "Package Server" > "Firmware Backup" > "Auto Update Feature" Menu.....	220
Table 167: "Package Server" > "Firmware Restore" Menu	221
Table 168: "Package Server" > "Firmware Restore" > "Select Package" Menu	221
Table 169: "Package Server" > "System Partition" Submenu	222
Table 170: "Mass Storage" Menu	223
Table 171: "Mass Storage" > "SD Card" Menu	223
Table 172: "Ports and Services" Menu	225
Table 173: "Ports and Services" > "Telnet" Submenu	226
Table 174: "Ports and Services" > "FTP" Submenu.....	226
Table 175: "Ports and Services" > "FTPS" Submenu	227
Table 176: "Ports and Services" > "HTTP" Submenu	227
Table 177: "Ports and Services" > "HTTPS" Submenu.....	228
Table 178: "Ports and Services" > "NTP" Submenu	228
Table 179: "Ports and Services" > "SSH" Submenu	229
Table 180: "Ports and Services" > "TFTP" Submenu	229
Table 181: "Ports and Services" > "DHCPD" Submenu.....	230
Table 182: "Ports and Services" > "DHCPD" > "Xn" Submenu.....	230
Table 183: "Ports and Services" > "DNS" Submenu.....	231
Table 184: "Ports and Services" > "IOCHECK PORT" Submenu	232
Table 185: "Ports and Services" > "Modbus TCP" Submenu	232
Table 186: "Ports and Services" > "Modbus UDP" Submenu	233
Table 187: "Ports and Services" > "OPC UA" Submenu.....	233
Table 188: "Ports and Services" > "Firewall Status" Submenu	234

Table 189: "Ports and Services" > "PLC Runtime Services" Submenu	235
Table 190: "Ports and Services" > "PLC Runtime Services" > "e!RUNTIME" Submenu	235
Table 191: "SNMP" Menu	236
Table 192: "SNMP" > "General SNMP Configuration" Submenu	236
Table 193: "SNMP" > "SNMP v1/v2c Manager Configuration" Submenu	237
Table 194: "SNMP" > "SNMP v1/v2c Trap Receiver Configuration" Submenu	237
Table 195: "SNMP" > "SNMP v3 Configuration" Submenu	238
Table 196: "SNMP" > "(Secure)SNMP firewalling" Submenu	239
Table 197: CODESYS V3 Priorities	248
Table 198: WAGO Modbus Registers	251
Table 199: Watchdog Commands	255
Table 200: Watchdog Status	256
Table 201: Watchdog Configuration	257
Table 202: System Power Supply Diagnostics	262
Table 203: Field-Side Supply Diagnostics	262
Table 204: Diagnostics via SYS LED	263
Table 205: RUN LED Diagnostics	264
Table 206: Diagnostics I/O LED	265
Table 207: MS-LED Diagnostics	266
Table 208: BT-LED Diagnostics	267
Table 209: LNK-LED Diagnostics	268
Table 210: ACT-LED Diagnostics	268
Table 211: Overview of Error Codes, I/O LED	272
Table 212: Error Code 1, Explanation of Blink Codes and Procedures for Troubleshooting	273
Table 213: Error Code 2, Explanation of Blink Codes and Procedures for Troubleshooting	274
Table 214: Error Code 3, Explanation of Blink Codes and Procedures for Troubleshooting	275
Table 215: Error Code 4, Explanation of Blink Codes and Procedures for Troubleshooting	276
Table 216: Error Code 5, Explanation of Blink Codes and Procedures for Troubleshooting	276
Table 217: Error Code 7, Explanation of Blink Codes and Procedures for Troubleshooting	276
Table 218: Error Code 9, Explanation of Blink Codes and Procedures for Troubleshooting	277
Table 219: Overview of MS-LED Error Codes	278
Table 220: Error Code 1, Explanation of Blink Codes and Procedures for Troubleshooting	278
Table 221: Description of Marking Example According to ATEX and IECEx	290
Table 222: Description of Marking Example for Approved Ex i I/O Module According to ATEX and IECEx	292
Table 223: Description of Marking Example According to NEC 500	293
Table 224: Description of Marking Example for Approved Ex i I/O Module According to NEC 505	294
Table 225: Description of Marking Example for Approved Ex i I/O Modules According to NEC 506	294

Table 226: Description of Marking Example for Approved Ex i I/O Modules According to CEC 18 attachment J	295
Table 227: 1 Channel Digital Input Module with Diagnostics	300
Table 228: 2 Channel Digital Input Modules	300
Table 229: 2 Channel Digital Input Module with Diagnostics	300
Table 230: 2 Channel Digital Input Module with Diagnostics and Output Process Data	301
Table 231: 4 Channel Digital Input Modules	301
Table 232: 8 Channel Digital Input Modules	301
Table 233: 8 Channel Digital Input Module NAMUR with Diagnostics and Output Process Data	302
Table 234: 8 Channel Digital Input Module PTC with Diagnostics and Output Process Data	303
Table 235: 16 Channel Digital Input Modules	304
Table 236: 1 Channel Digital Output Module with Input Process Data	305
Table 237: 2 Channel Digital Output Modules	305
Table 238: 2 Channel Digital Input Modules with Diagnostics and Input Process Data	306
Table 239: 2 Channel Digital Input Modules with Diagnostics and Input Process Data 75x-506	306
Table 240: 4 Channel Digital Output Modules	307
Table 241: 4 Channel Digital Output Modules with Diagnostics and Input Process Data	307
Table 242: 8 Channel Digital Output Module	307
Table 243: 8 Channel Digital Output Modules with Diagnostics and Input Process Data	308
Table 244: 16 Channel Digital Output Modules	308
Table 245: 8 Channel Digital Input/Output Modules	309
Table 246: 1 Channel Analog Input Modules	310
Table 247: 2 Channel Analog Input Modules	310
Table 248: 2-Channel Analog Input Modules HART	312
Table 249: 2 Channel Analog Input Modules HART + 6 bytes Mailbox	312
Table 250: 4 Channel Analog Input Modules	312
Table 251: 8 Channel Analog Input Modules	313
Table 252: 3-Phase Power Measurement Module	314
Table 253: 3-Phase Power Measurement Modules 750-494, -495, (and all variations)	315
Table 254: 2 Channel Analog Output Modules	316
Table 255: 4 Channel Analog Output Modules	316
Table 256: Counter Modules 750-404, (and all variations except of /000-005), 753-404, -404/000-003	317
Table 257: Counter Modules 750-404/000-005, 753-404/000-005	318
Table 258: Counter Modules 750-633	319
Table 259: Counter Modules 750-638, 753-638	319
Table 260: Pulse Width Modules 750-511, /xxx-xxx, 753-511	320
Table 261: Serial Interface Modules with Alternative Data Format	321
Table 262: Serial Interface Modules with Standard Data Format	321
Table 263: Serial Interface Modules 750-652, 753-652	322
Table 264: Data Exchange Module 750-654, -654/000-001	322
Table 265: SSI Transmitter Interface Modules	323

Table 266: SSI Transmitter Interface I/O Modules with an Alternative Data Format (/000-004, -005, -007).....	323
Table 267: Incremental Encoder Interface Modules 750-631/000-004, --010, -011.....	323
Table 268: Incremental Encoder Interface Modules 750-634.....	324
Table 269: Incremental Encoder Interface Modules 750-637, (and all variations).....	324
Table 270: Digital Pulse Interface Modules 750-635, 753-635.....	325
Table 271: DC-Drive Controller 750-636, -636/000-700, -636/000-800	325
Table 272: Stepper Controller 750-670, -671, -672	326
Table 273: RTC Module 750-640	327
Table 274: DALI Multi-Master Module 753-647 in the "Easy" Mode.....	328
Table 275: DALI Multi-Master Module 753-647 in the "Full" Mode.....	330
Table 276: LON® FTT Module 753-648	331
Table 277: EnOcean Radio Receiver 750-642	331
Table 278: MP Bus Master Module 750-643	332
Table 279: <i>Bluetooth</i> ® RF-Transceiver 750-644	333
Table 280: Vibration Velocity/Bearing Condition Monitoring VIB I/O 750-645...	333
Table 281: KNX/EIB/TP1 Module 753-646	334
Table 282: AS-interface Master Module 750-655, 753-655	335
Table 283: System Modules with Diagnostics 750-606, -611	336
Table 284: System Modules with Diagnostics 750-610, -611	336
Table 285: Filter Modules 750-624/020-002, 750-626/020-002	336
Table 286: Binary Space Module 750-622 (with Behavior like 2 Channel Digital Input)	337



WAGO Kontakttechnik 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