

WAGO I/O System Compact



751-9401 **Compact Controller 100**

© 2024 WAGO GmbH & Co. KG
All rights reserved.

WAGO GmbH & Co. KG

Hansastraße 27
D-32423 Minden

Phone: +49 (0) 571/8 87 – 0
Fax: +49 (0) 571/8 87 – 844 169

E-Mail: info@wago.com

Web: www.wago.com

Technical Support

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

E-Mail: support@wago.com

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

E-Mail: documentation@wago.com

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

WAGO is a registered trademark of WAGO Verwaltungsgesellschaft mbH.

Table of Contents

1	Notes about this Documentation	9
1.1	Validity of this Documentation	9
1.2	Copyright	9
1.3	Property rights	10
1.4	Symbols	12
1.5	Number Notation	14
1.6	Font Conventions	14
2	Important Notes	15
2.1	Legal Bases	15
2.1.1	Subject to Changes	15
2.1.2	Personnel Qualifications	15
2.1.3	Intended Use	15
2.1.4	Technical Condition of Specified Devices	16
2.2	Safety Advice (Precautions)	17
2.3	Licensing Terms of the Software Package Used	20
2.4	Special Use Conditions for ETHERNET Devices	21
3	Overview	22
4	Properties	25
4.1	Hardware Description	25
4.1.1	View	25
4.1.2	Labeling and type plate	27
4.1.3	Connectors	29
4.1.3.1	Network Connectors	29
4.1.3.2	Service Interface	29
4.1.3.3	Supply voltage	29
4.1.3.4	Digital inputs and outputs	29
4.1.3.4.1	Digital inputs	29
4.1.3.4.2	Digital outputs	30
4.1.3.5	Analog inputs and outputs	31
4.1.3.5.1	Analog inputs	31
4.1.3.5.2	Analog outputs	32
4.1.3.6	Communication Interface	32
4.1.3.6.1	Operating as an RS-485 Interface	33
4.1.3.7	CAN Interface	33
4.1.3.8	Analog Temperature Sensors	36
4.1.4	Display Elements	37
4.1.4.1	System LEDs	37
4.1.4.2	Network Connection LED	37
4.1.4.3	Memory Card Slot LED	37
4.1.4.4	Status DI/DO LEDs	37
4.1.4.5	CAN LED	37
4.1.5	Operating Elements	38
4.1.5.1	Operating Mode Switch	38
4.1.5.2	Reset Button	38
4.1.6	Memory Card Slot	39

4.2	Schematic Diagram	40
4.3	Technical Data	41
4.3.1	Mechanical Data	41
4.3.2	System Data	41
4.3.3	Power Supply.....	41
4.3.4	Clock.....	42
4.3.5	Programming	43
4.3.6	ETHERNET	43
4.3.7	CANopen	44
4.3.8	Communication Interface	44
4.3.9	Connection Type.....	45
4.3.10	Digital inputs	45
4.3.11	Digital outputs	46
4.3.12	Analog inputs	46
4.3.13	Analog outputs.....	46
4.3.14	Climatic Environmental Conditions.....	47
4.3.15	Analog Temperature Sensors	48
4.3.16	Fieldbus	48
4.3.17	Other.....	48
4.4	Approvals	49
4.5	Standards and Guidelines	49
5	Function Description	50
5.1	Network.....	50
5.1.1	Interface Configuration.....	50
5.1.1.1	Operation in Switch Mode.....	50
5.1.1.2	Operation with Separate Network Interfaces.....	50
5.1.1.3	MAC ID and IP Address Assignment Examples.....	52
5.1.2	Network Security.....	53
5.1.2.1	Users and Passwords.....	53
5.1.2.1.1	Services and Users.....	53
5.1.2.1.2	WBM User Group.....	54
5.1.2.1.3	Linux® User Group	54
5.1.2.1.4	SNMP User Group	55
5.1.2.2	Web Protocols for WBM Access	56
5.1.2.2.1	TLS Encryption	56
5.1.2.3	Root Certificates.....	58
5.1.3	Network Configuration.....	59
5.1.3.1	Host Name/Domain Name	59
5.1.3.2	Routing.....	59
5.1.4	Network Services	62
5.1.4.1	DHCP Client.....	62
5.1.4.2	DHCP Server.....	62
5.1.4.3	DNS Server	64
5.1.5	Cloud Connectivity Functionality	65
5.1.5.1	Components of the Cloud Connectivity Software Package	66
5.2	Memory Card Function	67
5.2.1	Formatting.....	67
5.2.2	Data Backup	68
5.2.2.1	Backup Function.....	68

5.2.2.2	Restore Function	69
5.2.3	Inserting a Memory Card during Operation	71
5.2.4	Removing the Memory Card during Operation	71
5.2.5	Setting the Home Directory for the Runtime System	72
5.2.6	Load Boot Project	72
6	Mounting.....	74
6.1	Installation Position.....	74
6.2	Mounting onto Carrier Rail	76
6.2.1	Carrier Rail Properties.....	76
6.2.2	WAGO DIN Rails	77
6.3	Spacing	77
6.4	Inserting Devices	79
6.4.1	Inserting the Controller.....	79
6.4.2	WAGO <i>picoMAX</i> ® Connectors	79
6.4.2.1	Status at delivery.....	80
6.4.2.2	Removing the Female Connector	80
6.4.2.2.1	Removing the Female Connector without Wiring.....	80
6.4.2.2.2	Removing the Female Connector with Wiring	81
6.4.2.3	Plugging in the Female Connector.....	82
7	Connecting	83
7.1	Earthing.....	83
7.2	Connecting Devices.....	83
7.3	Connecting the Power Supply.....	83
8	Commissioning	84
8.1	Switching On the Controller	84
8.2	Determining the IP Address of the Host PC	85
8.3	Setting an IP Address.....	86
8.3.1	IP Connection via USB.....	87
8.3.2	Changing an IP Address using “WAGO Ethernet Settings”	88
8.3.3	Temporarily Setting a Fixed IP Address	90
8.3.4	Setting the IP Address via the WBM	91
8.3.5	Assigning an IP Address using DHCP.....	92
8.4	Testing the Network Connection.....	93
8.5	Changing Passwords.....	94
8.6	Shutdown/Restart.....	95
8.7	Initiating Reset Functions	96
8.7.1	Warm Start Reset	96
8.7.2	Cold Start Reset.....	96
8.7.3	Software Reset	96
8.7.4	Controller Reset.....	96
8.8	Configuration	98
8.8.1	Configuration via Web-Based-Management (WBM).....	99
8.8.1.1	WBM User Administration.....	101
8.8.1.2	General Information about the Page.....	104
8.8.2	Configuration using “WAGO Ethernet Settings”.....	106
8.8.2.1	Identification Tab	108
8.8.2.2	Network Tab	109
8.8.2.3	PLC Tab	111

8.8.2.4	Status Tab	112
9	Run-time System CODESYS V3	113
9.1	General Notes	113
9.2	CODESYS V3 Priorities	114
9.3	Memory Spaces under CODESYS V3	115
9.3.1	Program and Data Memory	115
9.3.2	Function Block Limitation	115
9.3.3	Remanent Memory	115
9.3.4	File Access from the IEC Application	115
9.3.5	Changing Network Settings from the IEC Application	116
9.3.6	EtherCAT	116
9.4	Process Image	117
9.4.1	Analog Inputs	117
9.4.2	Analog outputs	117
9.4.3	Analog Temperature Inputs	118
9.4.4	Digital Inputs	118
9.4.5	Digital Outputs	119
10	CANopen Master and Slave	120
10.1	Object Directory	120
10.2	Communications Profile	121
10.2.1	Master Configuration	125
10.3	Data Exchange	127
10.3.1	Controller Communication Objects	127
10.3.2	Fieldbus-Specific Addressing	127
10.3.3	Examples for the Definition of PFC Fieldbus Variables	131
10.3.3.1	CODESYS Access to PFC Variables	131
10.3.3.2	Maximum Indices	132
10.3.4	Using the CANopen Slave (Device) under CODESYS V3	134
10.3.5	Use as a CAN Layer 2 Device	135
11	Diagnostics	136
11.1	Operating and Status Messages	136
11.1.1	"SYS" LED	136
11.1.1.1	SYS LED	136
11.1.1.2	RUN LED	136
11.1.1.3	CAN LED	137
11.1.2	Network Connection LED	138
11.1.2.1	"LNK ACT" LED	138
11.1.3	Memory Card Slot LED	139
12	Service	140
12.1	Inserting and Removing the Memory Card	140
12.1.1	Inserting the Memory Card	140
12.1.2	Removing the Memory Card	140
12.2	Firmware Changes	141
12.2.1	Use WAGOupload to Update/Downgrade the Firmware	142
12.2.2	Perform Firmware Update/Downgrade	143
12.3	Updating Root Certificates	144
13	Removal	145

13.1	Removing Devices.....	145
13.1.1	Remove Controller.....	145
14	Disposal.....	146
14.1	Electrical and electronic equipment	146
14.2	Packaging.....	146
15	Accessories.....	148
15.1	Tools	148
16	Appendix	149
16.1	Configuration Dialogs	149
16.1.1	Web-Based-Management (WBM)	149
16.1.1.1	“Information” Tab.....	149
16.1.1.1.1	“Device Status” Page	149
16.1.1.1.2	“Vendor Information” Page.....	151
16.1.1.1.3	“PLC Runtime Information” Page	152
16.1.1.1.4	“WAGO Software License Agreement” Page	153
16.1.1.1.5	“Open Source Licenses” Page	154
16.1.1.1.6	“WBM Third Party License Information” Page	155
16.1.1.1.7	“Trademarks Information” Page	156
16.1.1.1.8	“WBM Version” Page	157
16.1.1.2	“Configuration” Tab.....	158
16.1.1.2.1	“PLC Runtime Configuration” Page.....	158
16.1.1.2.2	“TCP/IP Configuration” Page	160
16.1.1.2.3	“Ethernet Configuration” Page.....	162
16.1.1.2.4	Configuration of Host and Domain Name” Page	166
16.1.1.2.5	“Routing” Page.....	168
16.1.1.2.1	“Spanning Tree Protocol” Page.....	173
16.1.1.2.2	“Clock Settings” Page	176
16.1.1.2.3	“Create Bootable Image” Page.....	178
16.1.1.2.4	“Firmware Backup” Page	179
16.1.1.2.5	“Firmware Restore” Page.....	181
16.1.1.2.6	“Active System” Page	183
16.1.1.2.7	“Mass Storage” Page	184
16.1.1.2.8	“Software Uploads” Page	185
16.1.1.2.9	“Configuration of Network Services” Page	186
16.1.1.2.10	“Configuration of NTP Client” Page.....	188
16.1.1.2.11	“PLC Runtime Services” Page	189
16.1.1.2.12	“SSH Server Settings” Page	190
16.1.1.2.1	“DHCP Server Configuration” Page	191
16.1.1.2.2	“Configuration of DNS Server” Page	192
16.1.1.2.3	“Status overview” Page	193
16.1.1.2.4	“Configuration of Connection <n>” Page	194
16.1.1.2.5	“Configuration of General SNMP Parameters” Page	201
16.1.1.2.6	“Configuration of SNMP v1/v2c Parameters” Page	202
16.1.1.2.7	“Configuration of SNMP v3 Parameters” Page.....	204
16.1.1.2.1	“Commissioning Settings” Page	208
16.1.1.2.2	Page “Dock Settings”	209
16.1.1.2.3	“WBM User Configuration” Page.....	210
16.1.1.3	“Fieldbus” Tab	211

16.1.1.3.1	“OPC UA Configuration” Page	211
16.1.1.3.1	“BACnet Status” Page.....	213
16.1.1.3.2	“BACnet Configuration” Page.....	214
16.1.1.3.3	“BACnet Data Link” Page.....	216
16.1.1.3.4	“BACnet Storage Location” Page	218
16.1.1.4	“Security” Tab.....	220
16.1.1.4.1	“OpenVPN / IPsec Configuration” Page	220
16.1.1.4.2	“General Firewall Configuration” Page	222
16.1.1.4.3	“Interface Configuration” Page	223
16.1.1.4.4	“Configuration of MAC Address Filter” Page	226
16.1.1.4.5	“Configuration of User Filter” Page.....	228
16.1.1.4.6	“Certificates” Page	230
16.1.1.4.7	“Boot mode configuration” Page.....	231
16.1.1.4.8	“Security Settings” Page	232
16.1.1.4.9	“Advanced Intrusion Detection Environment (AIDE)” Page ...	233
16.1.1.4.10	“WAGO Device Access” Page.....	235
16.1.1.5	“Diagnostic” Tab	236
16.1.1.5.1	“Log Message Viewer” Page.....	236
16.1.1.5.2	“Download” Page	237
16.1.1.5.3	“Network Capture” Page	238
List of Figures		242
List of Tables		243

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 “Compact Controller 100” controller (751-9401).

1.2 Copyright

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

1.3 Property rights

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

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

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

1.4 Symbols



DANGER

Personal Injury!

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



DANGER

**Personal Injury Caused by Electric Current!**

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



WARNING

Personal Injury!

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



CAUTION

Personal Injury!

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

NOTICE

Damage to Property!

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



NOTICE

Damage to Property Caused by Electrostatic Discharge (ESD)!

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



Note

Important Note!

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



Information

Additional Information:

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

1.5 Number Notation

Table 1: Number Notation

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

1.6 Font Conventions

Table 2: Font Conventions

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

2.1.2 Personnel Qualifications

All sequences implemented on WAGO I/O System Compact 751 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 Intended Use

Controllers of the modular WAGO I/O System Compact 751 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 fulfills the requirements of protection type IP20 and is designed for use in dry interior spaces. 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)". Use without additional protective measures in environments within which dust, corrosive fumes, gases or ionized radiation can occur is considered improper use.

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. Please observe the installation regulations!

You will find the relevant information in the section "Device Description" > "Standards and Guidelines" in the manual for the used product.

2.1.4 Technical Condition of Specified Devices

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

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

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

2.2 Safety Advice (Precautions)

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



DANGER

Do not work on devices while energized!

All power sources to the device shall be switched off prior to performing any installation, repair or maintenance work.



DANGER

Install device in a suitable enclosure!

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

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



DANGER

Ensure disconnect and overcurrent protection!

The device is intended for installation in automation technology systems. Disconnect protection is not integrated. Connected systems must be protected by a fuse.

Provide suitable disconnect and overcurrent protection on the system side!



DANGER

Ensure a standard connection!

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

**WARNING****Power from SELV/PELV power supply only!**

All field signals and field supplies connected to the controller „Compact Controller 100“ (751-9401) must be powered from SELV/PELV power supply(s)!

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**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.

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.

2.3 Licensing Terms of the Software Package Used

The firmware for the “Compact Controller 100” controller (751-9401) contains open-source software.

The licence conditions of the software packages are stored in the controller in text form. They can be accessed via the WBM page “Legal Information” > “Open Source Software.”

You can obtain the source code with licensing terms of the open-source software from WAGO GmbH & Co. KG on request. Send your request to support@wago.com with the subject “Controller Board Support Package.”

2.4 Special Use Conditions for ETHERNET Devices

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

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

3 Overview

The controller 751-9401(Compact Controller 100) 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. Among other things, the controller has integrated digital and analog inputs and outputs and a serial onboard interface in accordance with EIA-485/RS-485.

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

Automation tasks can be executed in all IEC 61131-3-compatible languages with the CODESYS V3 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 32 MB of program memory (flash), 128 MB of data memory (RAM) as well as 128 kB of retentive memory (retain and flag variables in an integrated NVRAM).

Two ETHERNET interfaces and the integrated, configurable switch enable wiring in all necessary configurations with one common network where both ports share a common IP address or with two separate networks where each port has its own IP address.

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

Both of these interfaces support:

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

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

- Modbus TCP Client/Server
- Modbus RTU Master/Slave (via RS-485)
- Gateway Modbus TCP to Modbus RTU
- EtherCAT Master
- EtherNet/IP Adapter

- EtherNet/IP Scanner
- OPC UA
- CANopen Master/Slave

CODESYS V3 makes configuring the fieldbus possible.

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

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

- a SNMP server/client
- a FTP server, a FTPS server (explicit connections only)
- a SSH server/client
- a Web server
- a NTP client
- a BootP and DHCP client
- a DHCP server
- a DNS server
- a CODESYS V3 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 as it is suitable for industrial applications subjected to environmental extremes and for use in this device.

Compatibility with other commercially available storage media cannot be guaranteed.

4 Properties

4.1 Hardware Description

4.1.1 View

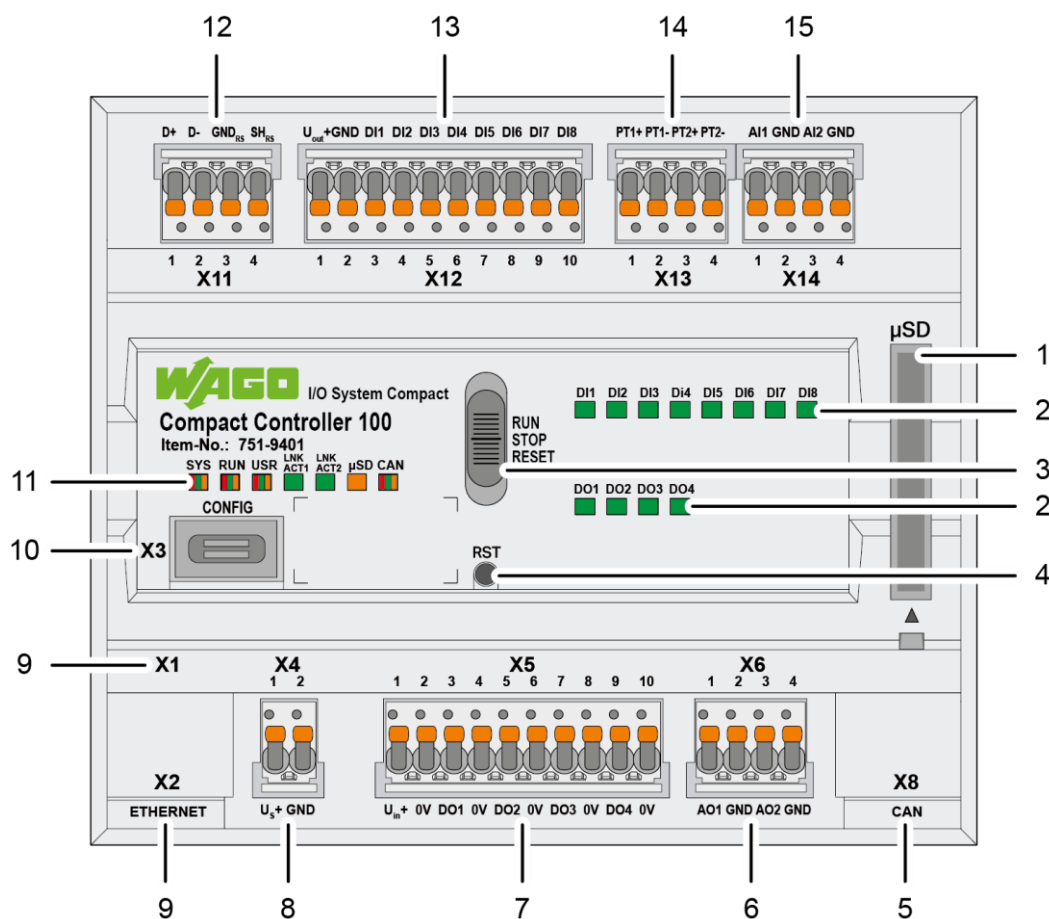


Figure 1: View




Table 3: Legend for figure "View"

Position	Description	See sector
1	Slot for memory card	"Memory Card Slot"
2	LED indicators – Status DI/DO	"Display Elements" > „Status DI/DO LEDs“
3	Operating Mode Switch	"Operating Elements" > "Operating Mode Switch"
4	Reset Button	"Operating Elements" > "Reset Button"
5	CAN Interface – "X8"	"Connectors" > "CAN Interface"
6	Analog outputs AO – "X6"	"Connectors" > "Analog inputs and outputs"
7	Digital outputs DO – "X5"	"Connectors" > "Digital inputs and outputs"
8	Supply voltage system – "X4"	"Connectors" > "Supply voltage"
9	Network connections ETHERNET – "X1", "X2"	"Connectors" > "Network Connectors"
10	Service interface – "X3"	"Connectors" > "Service Interface"
11	LED indicators – System / Network connections / Slot for memory card	"Display Elements" > > "System LEDs", "Display Elements" > "Network Connections LED", "Display Elements" > "Memory Card Slot LED", "Display Elements" > "CAN LED"
12	Communication interface RS-485 – "X11"	"Connectors" > "Communication Interface"
13	Digital inputs DI – "X12"	"Connectors" > "Digital inputs and outputs"
14	Analog Temperature Sensors – "X13"	"Connectors" > "Analog Temperature Sensors"
15	Analog inputs AI – "X14"	"Connectors" > "Analog inputs and outputs"

4.1.2 Labeling and type plate

The labeling and the type plate are attached to the left side of the product. The following information is included in it:

Table 4: Labeling and type plate

Field	Example
Item description	Compact Controller 100
Series	I/O System Compact
Item Number	Item-No.: 751-9401
QR code	
Power consumption System	$20.4\text{ V} \leq U_s + \leq 28.8\text{ V} / \text{max.} 0.5\text{ A}$
Power consumption Field (Digital Outputs)	$20.4\text{ V} \leq U_{in} + \leq 28.8\text{ V} / \text{max.} 2\text{ A}$
Power consumption System supply	$20.4\text{ V} \leq U_{out} + \leq 28.8\text{ V} / \text{max.} 0.2\text{ A}$
Surrounding air temperature (operation)	$-25\text{ °C} \leq T_{amb} \leq + 60\text{ °C}$
Serial number	UN31564010260470190+ 0000000002342273
Control number	21110.5003
Date of manufacture (year – month) and Hardware revision number	2021-09-14
Data matrix code	
Barcode	

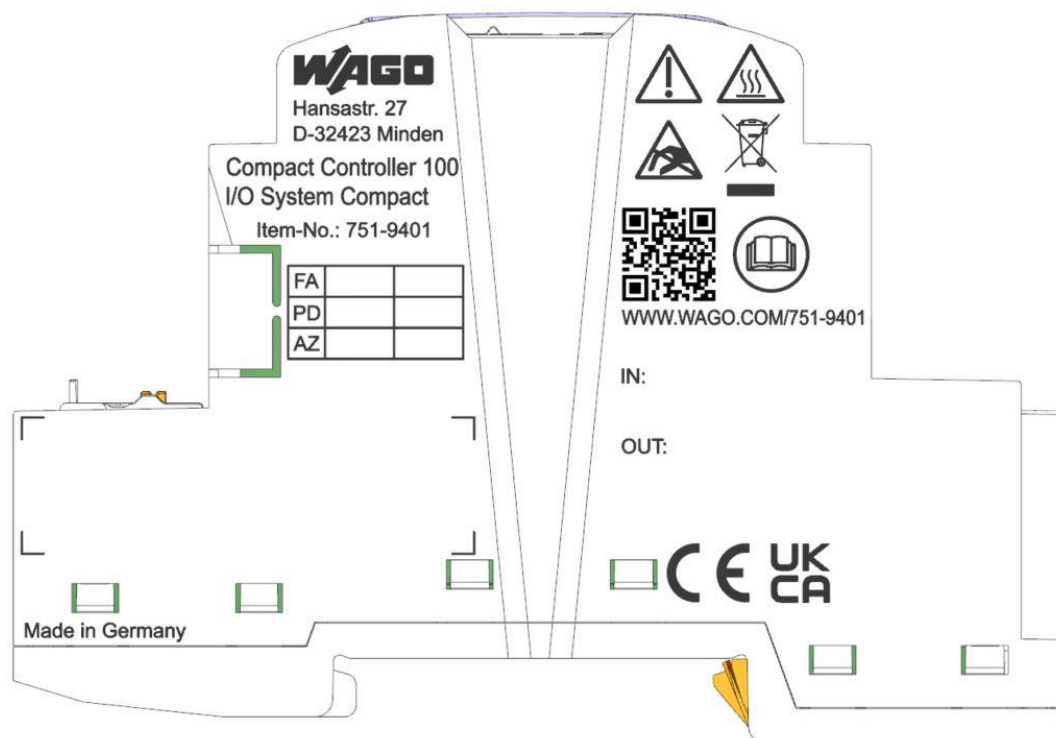


Figure 2: Labeling (Example)

SN: (37S)
UN315640102
60470190+
0000000002342273

21110.5003
2021-09-14



Figure 3: Type plate (Example)

4.1.3 Connectors

4.1.3.1 Network Connectors

Table 5: Network Connections ETHERNET – “X1”, “X2”

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

4.1.3.2 Service Interface

The service interface „X3“ is used for the communication with WAGO Ethernet Settings.

You can establish an IP connection via the USB service interface for commissioning and for service purposes, see also chapter “Commissioning” > “Setting an IP Address” > “IP Connection via USB”.

The USB service interface is designed as a USB-C socket. The interface supports USB Specification 2.0.

The controller appears on the host device (PC) as a peripheral device in device mode.

4.1.3.3 Supply voltage

Table 6: Supply Voltage – “X4”

Contact	Signal	Description
1	U _S +	Supply voltage
2	GND	Ground

4.1.3.4 Digital inputs and outputs

The connectors are for connecting actuators and sensors.
picoMAX® plugs with push-in CAGE CLAMP®S connections are used.

4.1.3.4.1 Digital inputs

The controller receives binary control signals from digital field devices (e.g., sensors, encoders, switches or proximity switches).

The product has 8 input channels (8DI, 24 VDC, 2.8 mA).

Each input channel has a noise-rejection RC filter with a 5.0 μ s time constant.

The inputs provide high-side switching. If the 24V potential for system power U_{out+} ("X12" connector) is switched to an input connection, the signal status for the corresponding input channel is set to "high".

A green status LED for each channel indicates the signal status.

The meaning of the LEDs is described in Section "Display Elements" > "LEDs Status DI/DO".

Table 7: Digital inputs – "X12"

Contact	Signal	Description
1	U_{out+}	Supply voltage output (DI1 ... DI8)
2	GND	Ground
3	DI1	Digital input 1
4	DI2	Digital input 2
5	DI3	Digital input 3
6	DI4	Digital input 4
7	DI5	Digital input 5
8	DI6	Digital input 6
9	DI7	Digital input 7
10	DI8	Digital input 8



Note

Attention — potential!

The supply voltage output U_{out+} /GND is not short-circuit protected.

4.1.3.4.2 Digital outputs

The controller transmits binary control signals from an automation device to connected actuators (e.g., magnetic valves, contactors, transmitters, relays or other electrical loads).

The product has 4 output channels (4DO, 24 VDC, 0.5 A).

The outputs provide high-side switching. If the signal status of an output channel is at "high", the 24V potential for field power is switched to the appropriate output channel.

The field supply is used to supply the Digital Outputs.

A green status LED for each channel indicates the signal status.

The meaning of the LEDs is described in Section "Display Elements" > "LEDs Status DI/DO".

The field level of the Digital Outputs are electrically isolated from the system level.

The connections are specified per EN 61010-2-201:
DC, general use

Table 8: Digital outputs – “X5”

Contact	Signal	Description
1	U _{in} +	Supply voltage input (DO1 ... DO4)
2	0V	Ground
3	DO1	Digital output 1
4	0V	Ground
5	DO2	Digital output 2
6	0V	Ground
7	DO3	Digital output 3
8	0V	Ground
9	DO4	Digital output 4
10	0V	Ground

4.1.3.5 Analog inputs and outputs

The connectors are for connecting actuators and sensors.
picoMAX® plugs with push-in CAGE CLAMP®S connections are used.

4.1.3.5.1 Analog inputs

The controller processes signals with standardized values of 0 ... +10 V from the field range.

The product has 2 input channels for field signals.

The sensors are connected to AI1 and ground or AI2 and ground in each case.

The ground connections are available for both channels on a common 0V ground potential.

The input signal is transmitted at a resolution of 16 bits.

The internal power supply powers the module.

Table 9: Analog inputs – “X14”

Contact	Signal	Description
1	AI1	Analog input 1
2	GND	Ground
3	AI2	Analog input 2
4	GND	Ground

4.1.3.5.2 Analog outputs

The controller generates signals with standardized values of 0 ...+10 V for the field range.

The product has 2 output channels, making two 2-wire actuators possible.

The actuators are connected via the AO1 and ground connections or AO2 and ground.

The channels have a common ground potential.

The output signal is output at a resolution of 12 bits.

The internal power supply powers the module.

Table 10: Analog outputs – “X6”

Contact	Signal	Description
1	AO1	Analog output 1
2	GND	Ground
3	AO2	Analog output 2
4	GND	Ground

4.1.3.6 Communication Interface

The communication interface integrated in the controller allows devices with an RS-485 interface to be connected.

The D +, D-, GND_{RS} and SH_{RS} connections are used for wiring to the communication partner.

The shield connection directly connects to the DIN-rail.

The interface operates in accordance with DIN 66259.

The connected device can communicate directly via the controller used. The active communication channel works independently of the higher-level bus system in half-duplex mode at up to 115200 baud.

The RS-485 interface guarantees a high level of interference immunity through differential transmission and electrically isolated signals.

Table 11: Communication Interface RS-485 – “X11”

Contact	Signal	Description
1	D+	Transmit/receive data +
2	D–	Transmit/receive data –
3	GND _{RS}	Ground
4	SH _{RS}	Shield

4.1.3.6.1 Operating as an RS-485 Interface

To minimize reflections at the end of the line, the RS-485 line must be terminated at the end at a line termination of 120 Ohm. The RS-485 line is already terminated in the Compact Controller 100 with a bus terminating resistor (120 Ohm). A bias network (pull-up and pull-down resistor) is also integrated in the Compact Controller 100 to keep the bus lines at a defined level when no other subscriber is active.

Note



Attention — bus termination!

The RS-485 bus must be terminated at the end!

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.

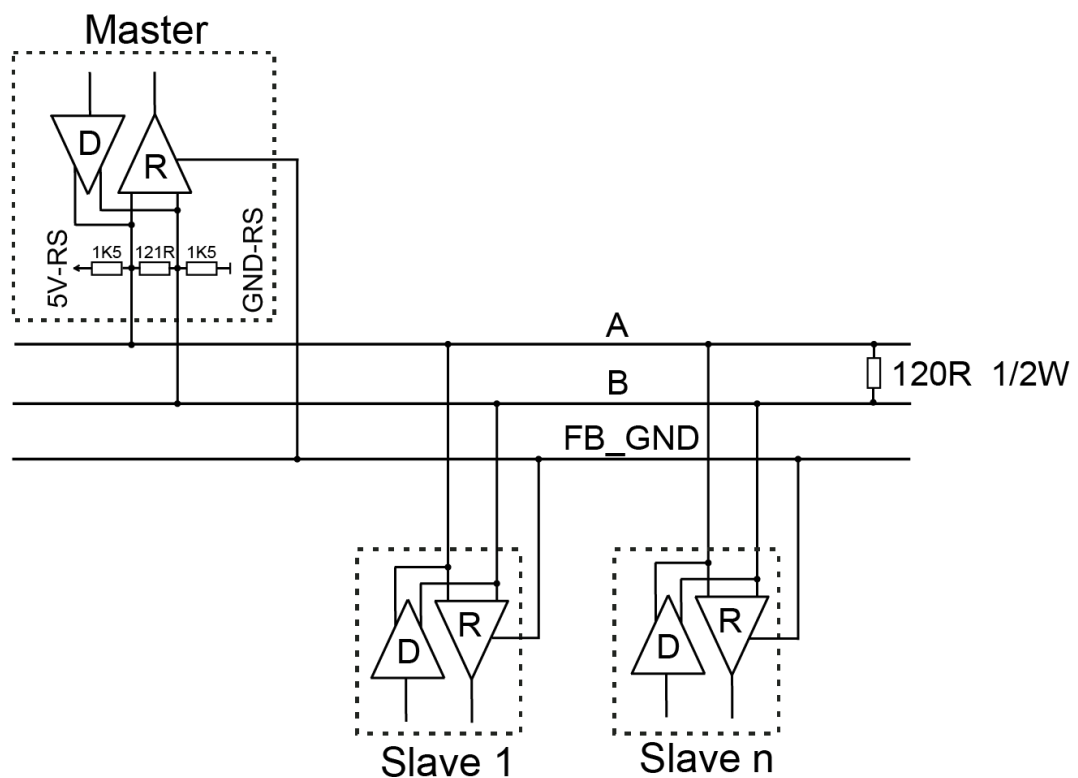


Figure 4: RS-485 Bus Termination

4.1.3.7 CAN Interface

The CAN interface is designed as an RJ-45 socket.

Table 12: CANopen Interface Pin Assignment – X8

Contact	Signal	Description
1	CAN_H	CAN Signal High
2	CAN_L	CAN Signal Low
3	GND	Ground
4	NC	Not assigned
5	NC	Not assigned
6	NC	Not assigned
7	NC	Not assigned
8	NC	Not assigned

DC/DC converters and optocouplers in the fieldbus interface provide electrical isolation between the CANopen bus system and the electronics.

The cable shield must be applied to the CAN shield. This is terminated to ground in devices with 1 M Ω (DIN rail contact). A low-impedance connection of the shielding to ground is possible only from the outside (e.g., by a supply module). We recommend using central ground contacts for the entire CANopen bus line shielding.

To minimize reflection at the end of the line, the CANopen line must be terminated at both ends by a cable termination.

Note



Attention - bus termination!

The CANopen bus segment must be terminated at both ends!
No more than 2 terminations per bus segment may be used!
Terminations may not be used in stub and branch lines!
Operation without proper termination of the CANopen network may result in transmission errors.

Note



Observe permissible resistor power loss!

For normal operation, 1/4 Watt resistors are sufficient. In the event of a short circuit (24 V power supply to a bus line), the resistor is subjected to a power loss of (short-circuit output current from transceiver \times power supply voltage). The resistor must be designed to withstand this power loss level.

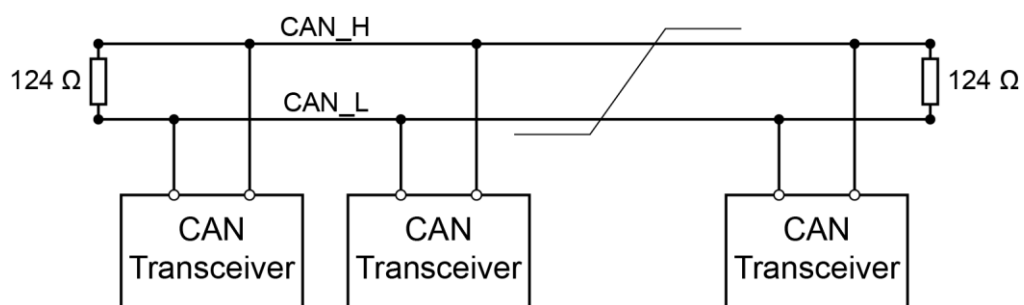


Figure 5: CANopen Standard Bus Termination

4.1.3.8 Analog Temperature Sensors

The connections are used to connect actuators and sensors.

picoMAX® plugs with Push-in CAGE CLAMP® Connections are used.

Analog temperature sensors such as Pt1000 or Ni1000 can be connected to the controller.

The resistance values are converted into temperature values. A microprocessor linearizes the measured resistance values and converts them into a numeric value proportional to the temperature of the selected resistance sensor.

The controller has 2 input channels, providing a direct connection to 2-wire resistance sensors.

Table 13: Analog Temperature Sensors – “X13”

Contact	Signal	Description
1	PT1+	Analog input Pt1000/Ni1000
2	PT1–	
3	PT2+	
4	PT2–	

4.1.4 Display Elements

4.1.4.1 System LEDs

Table 14: System LEDs

Designation	Color	Description
SYS	Red/Green/Off	System Status
RUN	Red/Green/Off	PLC program status
USR	Red/Green/Off	User LED, programmable using function blocks from the WAGO libraries to control the LEDs

4.1.4.2 Network Connection LED

Table 15: "LNK ACT" LEDs

Designation	Color	Description
LNK ACT1 LNK ACT2	Green/Off	ETHERNET connection status/data exchange

4.1.4.3 Memory Card Slot LED

Table 16: Memory Card Slot LED

Designation	Color	Description
μSD	Orange/Off	Memory card status

4.1.4.4 Status DI/DO LEDs

Table 17: Status DI/DO LEDs

Designation	Color	Description
DI1 ... DI8 DO1 ... DO4	Green/Off	Status Digital inputs and outputs

4.1.4.5 CAN LED

Table 18: CAN LED Indicator

Designation	Color	Description
CAN	Red/Green/ Orange/Off	Status CAN

4.1.5 Operating Elements

4.1.5.1 Operating Mode Switch

Table 19: Mode Selector Switch

Position	Actuation	Function
RUN	Latching	Normal operation CODESYS V3 applications running.
STOP	Latching	Stop All CODESYS V3 applications have stopped.
RESET	Spring-return	Reset warm start or Reset cold start (depending on length of actuation, see Section “Starting” > “Initiating Reset Functions”)

Other functions can also be initiated using the reset button.

4.1.5.2 Reset Button

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

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

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

4.1.6 Memory Card Slot

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 as it is suitable for industrial applications subjected to environmental extremes and for use in this device.

Compatibility with other commercially available storage media cannot be guaranteed.

4.2 Schematic Diagram

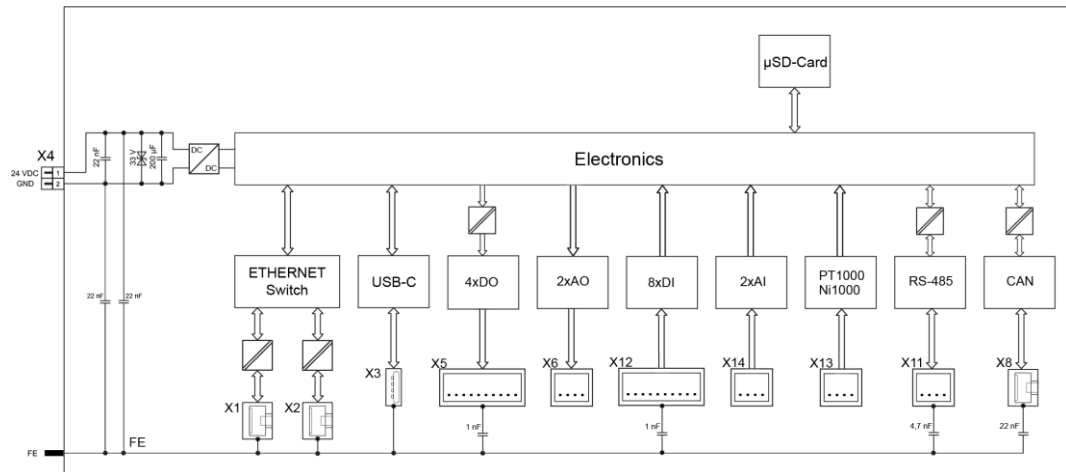


Figure 6: Schematic diagram

4.3 Technical Data

4.3.1 Mechanical Data

Table 20: Technical Data – Mechanical Data

Width	108 mm / 4.252 inch
Height	90 mm / 3.543 inch
Depth from upper edge of DIN-rail	55 mm / 2.165 inch
Weight	206 g

4.3.2 System Data

Table 21: Technical Data – System Data

CPU	2 × Cortex A7, 650 MHz
Operating System	Real-time Linux® with RT Preemption Patch
Memory card slot	Push-push mechanism, sealable cover lid
Type of memory card	MicroSD up to 32 Gbytes (All guaranteed properties are valid only in connection with the WAGO memory cards 758-879/000-3102 and 758-879/000-3108.)

4.3.3 Power Supply

Table 22: Technical Data – Power Supply

Input Voltage System U_{S+}	24 VDC (SELV, –15 ... +20 %) • Power supply via wiring interface (<i>picoMAX</i> ® connection)
Power consumption max. System U_{S+}	500 mA
Input voltage Field (Digital Outputs) U_{in+}	24 VDC (–15 ... +20 %) • Power supply via wiring interface (<i>picoMAX</i> ® connection)
Power consumption max. Field (Digital Outputs) U_{in+}	2 A
Output voltage System U_{out+}	24 VDC (–15 ... +20 %), not short-circuit protected
Current output max. System U_{out+}	200 mA
Isolation	1250 V (DC 1 min., between system level and field level (Digital Outputs))
Power failure time acc. IEC 61131-2	Depending on external buffering
Power loss at 35 °C	
Normal Operation	3,12 W
Full load (according to the technical data)	4,61 W

Note



Buffer for system power supply!

The system power supply and, if necessary, the field supply must be buffered to bridge power outages.

As the power demand depends on the respective node configuration, buffering is not implemented internally.

To achieve power outages of 1 ms to 10 ms according to IEC61131-2, determine the buffering appropriate for your node configuration and structure it as an external circuit.

4.3.4 Clock

Table 23: Technical Data – Clock

Buffer time RTC (25 °C)	6 days
-------------------------	--------

4.3.5 Programming

Table 24: Technical Data – Programming

Programming	CODESYS V3
IEC 61131-3	LD, FBD, ST, FC
Memory configuration	
Program memory (flash)	32 MByte
Data memory (RAM)	128 MByte
Non-volatile memory (NVRAM, Retain + Flags)	128 kByte

4.3.6 ETHERNET

Table 25: Technical Data – ETHERNET

ETHERNET	2 x RJ-45 (switched or separated mode)
Transmission medium	Twisted Pair S-UTP, 100 Ω, Cat 5, 100 m maximum cable length
Baud rate	10/100 Mbit/s; 10Base-T/100Base-TX
Protocols	DHCP, DNS, SNTP, FTP, FTPS (only explicit connections), SNMP, HTTP, HTTPS, SSH, Modbus (TCP), EtherCAT Master, EtherNet/IP Adapter, EtherNet/IP Scanner, OPC UA

Note



No direct access from fieldbus to the process image for I/O modules!

Any data that is required from the OnBoard I/O process image must be explicitly mapped in the control program to the data in the fieldbus process image and vice versa! Direct access is not possible!

4.3.7 CANopen

Table 26: Technical Data – CANopen

CANopen input and output process image max.	2000 words
---	------------

Note



Adjust CAN baud rate if necessary!

The controller supports baud rates from 10 kbit/s up to 1000 kbit/s for the CAN bus (X8). In the event of communication errors in connection with longer cable lengths and a larger number of bus participants, reduce the baud rate!

Note



No direct access from fieldbus to the process image for I/O modules!

Any data that is required from the OnBoard I/O process image must be explicitly mapped in the control program to the data in the fieldbus process image and vice versa! Direct access is not possible!

4.3.8 Communication Interface

Table 27: Technical Data – Communication Interface

Interface	1 x serial interface per TIA/EIA 485, <i>picoMAX</i> ®
Protocols	depending on IEC program
Transmission channels	1 TxD / 1 RxD, half duplex
Baud rate	115200 Baud
Isolation	Yes

4.3.9 Connection Type

Table 28: Technical Data – Field Wiring

Wire connection	<i>picoMAX</i> ® 3.5; Push-in CAGE CLAMP®
Actuation type	Push-button
Connectable conductor materials	Copper
Conductor cross-section (solid/fine-stranded conductors)	0.2 ... 1.5 mm ² / 24 ... 14 AWG
Conductor cross-section (fine-stranded conductors); (with insulated ferrule with plastic collar)	0.25 ... 0.75 mm ²
Conductor cross-section (fine-stranded conductors); (with uninsulated ferrule with plastic collar)	0.25 ... 1.5 mm ²
Stripped lengths	8 ... 9 mm / 0.31 ... 0.35 inch
Temperature resistance of conductors	min. 70 °C

4.3.10 Digital inputs

Table 29: Technical Data – Digital Inputs

Number of digital inputs	8
Input type	Type 3 (IEC 61131-2), high-side switching
Input signal "0"	–3 ... +5 VDC
Input signal "1"	+11 ... +30 VDC
Input filter	5.0 µs
Input current (typ.)	2.8 mA

4.3.11 Digital outputs

Table 30: Technical Data – Digital Outputs

Number of digital outputs	4
Output voltage	24 VDC
Load types	DC, general use (according to UL 61010-2-201, paragraph 4.4.2.101)
Reverse voltage protection	Yes
Switching frequency (max.)	1 kHz
Output current max., 1 output	0.5 A, short-circuit protected

4.3.12 Analog inputs

Table 31: Technical Data – Analog Inputs

Number of analog inputs	2
Connection types	Single-ended
Input voltage, measurement range	0 ... 10 V
Input voltage (max.)	±30 V
Typ. input resistance	> 100 kΩ
Resolution	16 bits
Temperature coefficient	< ±0.01 % / K of full scale value

4.3.13 Analog outputs

Table 32: Technical Data – Analog Outputs

Number of analog outputs	2
Output voltage, measurement range	0 ... 10 V
Load impedance	> 5 kΩ
Typ. settling time	100 ms
Resolution	12 bit
Measurement error at 25 °C	< ±0.2 % of full scale value
Temperature coefficient	< ±0.005 % / K of full scale value

4.3.14 Climatic Environmental Conditions

Table 33: Technical Data – Climatic Environmental Conditions

Surrounding air temperature (operation)	-25 ... +60 °C
Surrounding air temperature (storage)	-25 ... +85 °C
Relative humidity (without condensation)	5 ... 95 %
Operating altitude above sea level	2000 m
Pollution degree	2
Overvoltage category	II
Protection type	IP20
Special conditions	<ul style="list-style-type: none"> • Ensure that additional measures for components are taken, which are used in an environment involving: <ul style="list-style-type: none"> – dust, caustic vapors or gases – ionizing radiation • The permissible temperature range of the connecting cable must be dimensioned based on the mounting position and current intensity, as the temperature of the terminal connection can be up to 25 °K above the maximum expected surrounding air temperature (at 10 A).

The permissible ambient temperatures in relation to the installation positions can be found in section "Mounting" > "Installation Position".

4.3.15 Analog Temperature Sensors

Table 34: Technical Data – Analog Temperature Sensors

Number of inputs	2
Sensor types	Switchable: Pt1000, Ni1000 or raw value (450 ... 4400 Ohm)
Temperature range	
Pt	–60 ... +350 °C
Ni	–60 ... +350 °C
Measuring current (typ.)	0.5 mA
Connection types	2-wire connection
Resolution (over entire range)	16 bits
Measuring accuracy Pt1000 at 25 °C	< ±0.5 % hardware-related
Measuring accuracy Ni1000 at 25 °C	< ±0.5 % hardware-related
Temperature coefficient	< ±0.02 % / K of full scale value

4.3.16 Fieldbus

Table 35: Technical Data – Fieldbus

Supported protocols (license-free)	Modbus TCP (Client/Server) acc. CODESYS, Modbus RTU (Master/Slave) acc. CODESYS, Cloud Connectivity (1st connection), EtherCAT Master, EtherNet/IP Adapter, EtherNet/IP Scanner, OPC UA, CANopen
Supported protocols (license required)	Cloud Connectivity (2nd connection per DRM), MQTT Sparkplug (per DRM), BACnet/IP (per DRM), Telecontrol (IEC 60870, IEC 61850, DNP3) (per DRM)
Supported gateways (license-free)	Gateway Modbus TCP to Modbus RTU acc. CODESYS

4.3.17 Other

Table 36: Technical Data – Other

Fire load	6.386 MJ
-----------	----------

4.4 Approvals

The following approvals have been granted to the “Compact Controller 100” controller (751-9401):



Conformity Marking



UK Conformity Assessed

4.5 Standards and Guidelines

The “Compact Controller 100” controller (751-9401) fulfills the following EMC standards:

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

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

5 Function Description

5.1 Network

5.1.1 Interface Configuration

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

The two interfaces and configurable switch enable wiring for:

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

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

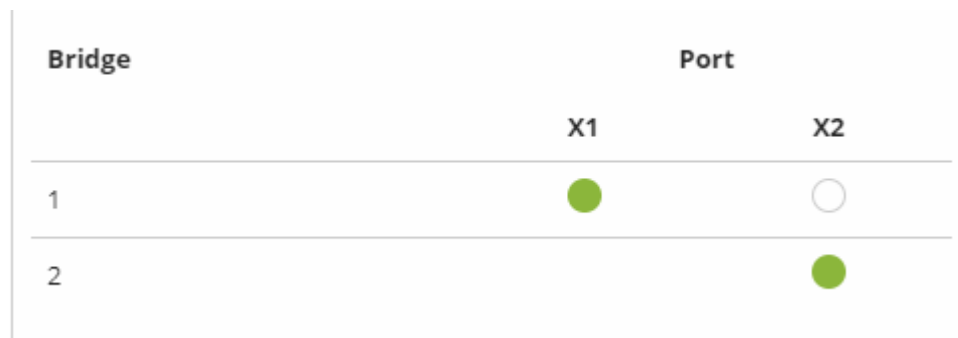


Figure 7: Example of Interface Assignment via WBM

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.

5.1.1.1 Operation in Switch Mode

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

When switching to Switch mode, the X1 settings are applied as a new common configuration for X1 and X2.

The device is then no longer accessible via the IP address previously set for X2. This must be taken into account for applications that use X2 for communication.

5.1.1.2 Operation with Separate Network Interfaces

When operating with separate network interfaces, both ETHERNET interfaces can be configured and used separately.

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

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

5.1.1.3 MAC ID and IP Address Assignment Examples

One common network with one common IP address for both ports

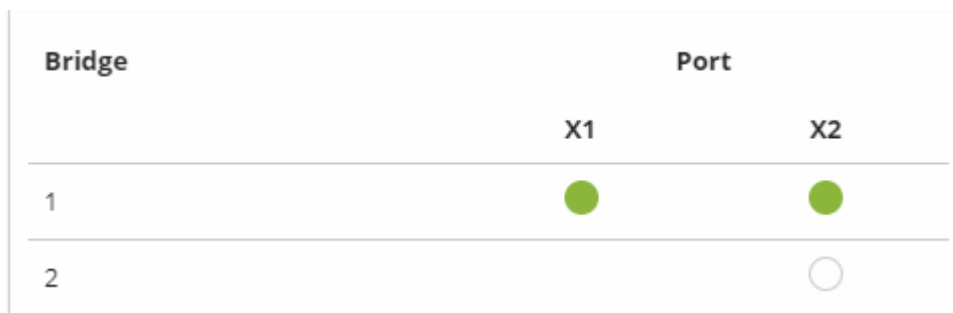


Figure 8: One Bridge with Two Ports

Table 37: MAC ID and IP Address Assignment for One Bridge with Two Ports

Bridge	MAC ID	IP Addr.	Port	MAC ID	Port	MAC ID
1	01	1	X1	02	X2	03

Two separate networks where each port has its own IP address



Figure 9: Two Bridges with One/One Ports

Table 38: MAC ID and IP Address Assignment for Two Bridges with One/One Ports

Bridge	MAC ID	IP Addr.	Port	MAC ID	Port	MAC ID
1	01	1	X1	01		
2	02	2			X2	02

5.1.2 Network Security

5.1.2.1 Users and Passwords

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

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



Note

Change passwords

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

5.1.2.1.1 Services and Users

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

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

5.1.2.1.2 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 39: WBM Users

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

Note



General Rights of WBM Users

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

Note



Change passwords

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

5.1.2.1.3 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 can be configured through a terminal connection.

Table 40: 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.

5.1.2.1.4 SNMP User Group

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

5.1.2.2 Web Protocols for WBM Access

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

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

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

5.1.2.2.1 TLS Encryption

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

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

The settings “Strong” and “Standard” are possible.

If “Strong” is set, the Webserver only allows TLS Version 1.2 and 1.3 and strong algorithms.

Older software and older operating systems may not support TLS 1.2 and TLS 1.3 and encryption algorithms.

If “Standard” is set, TLS 1.0, TLS 1.1, TLS 1.2 and TLS 1.3 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 or TLS 1.3

The German Federal Office for Information Security guidelines on migration to TLS 1.2 or TLS 1.3 contain “compatibility matrices” that show what software is comparable with TLS 1.2 or TLS 1.3.

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

5.1.2.3 Root Certificates

For communication encrypted with TLS, root certificates are used to verify the authenticity of the communication partner.

A root certificate, which is signed by a certificate authority, serves to verify the validity of all certificates issued by this certificate authority.

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

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

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

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

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

5.1.3 Network Configuration

5.1.3.1 Host Name/Domain Name

Without a host name configuration, the controller is assigned a default name which includes the last three values of the controller's MAC address. 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.

5.1.3.2 Routing

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

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

A routing entry consists of the following information:

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

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.

5.1.4 Network Services

5.1.4.1 DHCP Client

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

The following parameters can be obtained:

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

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

The Hostname and Domain parameters are each 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 stored.

5.1.4.2 DHCP Server

The controller provides the DHCP server service for the automatic configuration of IP addresses of network stations on the same subnet.

Generally, only one DHCP server can be active on a subnet at one time.

The following can be set for the DHCP server:

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

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

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

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

Table 41: List of Parameters Transmitted via DHCP

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

Not all parameters can be set in the WBM. If you want to set other values for the existing parameters or want to pass other parameters via DHCP, the DHCP

server must be manually configured. For the controller, the DHCP server service is handled by the program "dnsmasq".

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

5.1.4.3 DNS Server

The controller offers the DNS server service for the automatic assignment of hostnames to IP addresses of network stations.

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

The following settings are possible for the DNS server:

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

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

5.1.5 Cloud Connectivity Functionality

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

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

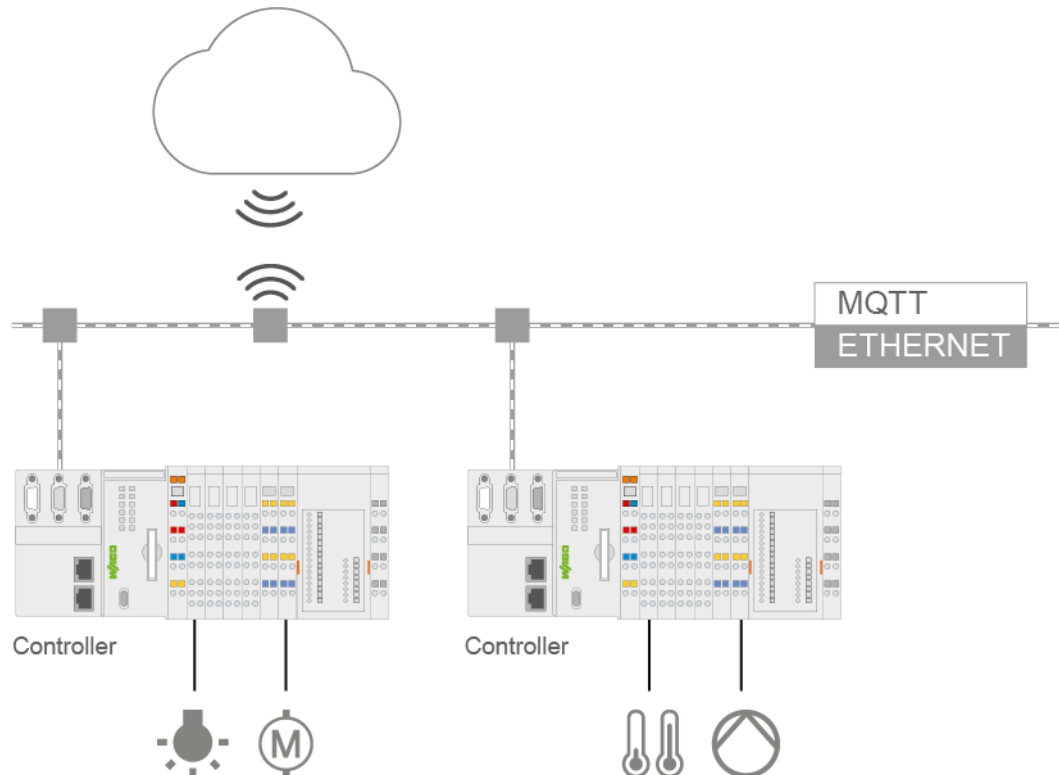


Figure 10: Connecting the Controller to a Cloud Service (Example)

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 “WagoAppCloud” library for CODESYS V3.

Note

**Please note the risks of using cloud services!**

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

Use encryption methods to protect your data and observe the information provided by the Federal Office for Information Security – “Cloud: Risks and Security Tips”.

Observe comparable publications of the competent, public institutions of your country.

Information

**Observe the additional documentation!**

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

Information

**Observe the necessary data protection and security settings!**

Before using the cloud connectivity functionality, consult the corresponding handbook and familiarize yourself with data protection and security issues.

You will find this in the Downloads area at www.wago.com.

5.1.5.1 Components of the Cloud Connectivity Software Package

Table 42: Components of the Cloud Connectivity Software Package

Components	Description
CODESYS V3: WagoAppCloud	IEC library to create the PLC application; function blocks make it possible to exchange data between the PLC and cloud service. The data transmission variables are definable.

5.2 Memory Card Function



Note

Only use recommended memory card!

Use only the SD memory card available from WAGO as it is suitable for industrial applications subjected to environmental extremes and for use in this device.

Compatibility with other commercially available storage media cannot be guaranteed.

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

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

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

5.2.1 Formatting



Note

Note the pre-formatting of the memory card!

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

5.2.2 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 “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, CODESYS settings)
- 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.

5.2.2.1 Backup Function

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

The backup function can be called via the WBM page “Firmware Backup”.

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

The files of the internal drive are stored on the target medium in the directory media/sd/copy and in the corresponding subdirectories.

The information that is not present as files on the controller is stored in XML format in the directory media/sd/settings/.

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

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

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

Note



Only one package may be copied to the network!

If you have specified "Network" as the storage location, only one package may be selected for each storing process.

Note



No backup of the memory card!

Backup from the memory card to the internal flash memory is not possible.

Note



Account for backup time

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

5.2.2.2 Restore Function

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

The restore function can be called via the WBM page "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.

5.2.3 Inserting a Memory Card during Operation

The fieldbus nodes and the PLC program are running.

Insert a memory card during ongoing operation.

During normal operation, the memory card is incorporated into the file system of the controller as a drive.

No automatic copy procedures are triggered.

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

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

5.2.4 Removing the Memory Card during Operation

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

Remove the memory card during ongoing operation.



Note

Data can be lost during writing!

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

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

The controller then works without a memory card.

5.2.5 Setting the Home Directory for the Runtime System

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

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

This setting can be activated using the check box "Home directory on memory card enabled" on the WBM page "PLC Runtime". Click the **[Submit]** button to apply the setting, which takes effect after the next restart.

No files are applied from the old to the new home directory.

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

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

Switching the home directory has no effect if the controller was 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.

5.2.6 Load Boot Project

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

Table 43: Loading a Boot Project

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

6 Mounting

6.1 Installation Position

Depending on the installation position and distance (D) of the product to the power supply (see chapter "Mounting">"Spacing"), different permissible ambient temperatures result.

The following installation positions are permitted:

Table 44: Installation positions and permitted ambient temperatures

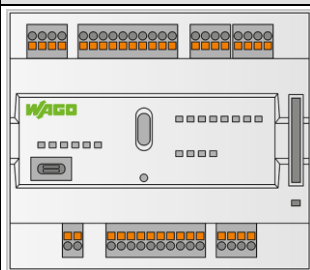
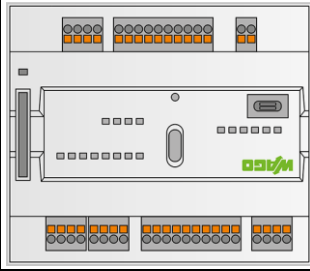
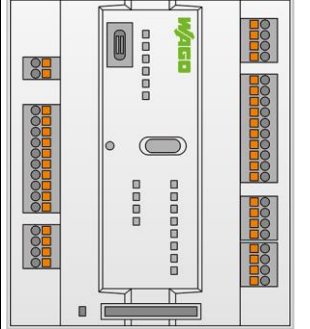
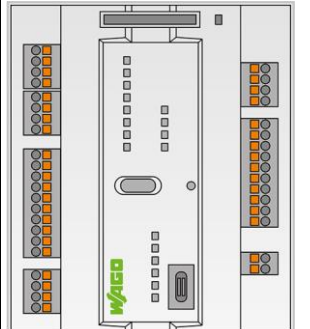
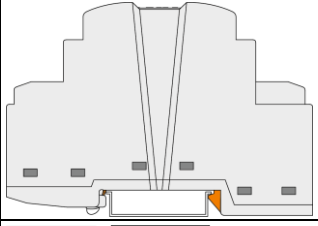
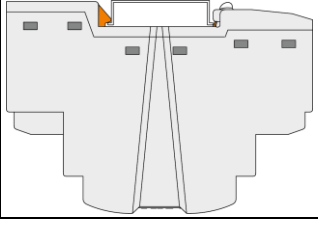
Figure	Installation position	Permitted ambient temperature
	Horizontal (standard)	D = 10 mm: –25 ... +60 °C D = 0 mm: –25 ... +55 °C
	Horizontal 180 °	D = 0 mm: –25 ... +55 °C
	Vertical	D = 0 mm: –25 ... +55 °C
	Vertical 180 °	D = 0 mm: –25 ... +50 °C

Table 44: Installation positions and permitted ambient temperatures

Figure	Installation position	Permitted ambient temperature
	Bottom mounting	D = 0 mm: -25 ... +50 °C
	Overhead mounting	D = 0 mm: -25 ... +50 °C

Note



Use an end stop in the case of vertical mounting!

In the case of vertical assembly, an end stop has to be mounted as an additional safeguard against slipping.

WAGO order no. 249-116 End stop for DIN 35 rail, 6 mm wide

WAGO order no. 249-117 End stop for DIN 35 rail, 10 mm wide

6.2 Mounting onto Carrier Rail

6.2.1 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 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 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 connections.
- A sufficiently stable carrier rail should be selected and, if necessary, several mounting points (every 20 cm) should be used in order to prevent bending and twisting (torsion).
- The geometry of the carrier rail must not be altered in order to secure the safe hold of the components. In particular, when shortening or mounting the carrier rail, it must not be crushed or bent.
- The base of the I/O components extends into the profile of the carrier rail. For carrier rails with a height of 7.5 mm, mounting points are to be riveted under the node in the carrier rail (slotted head captive screws or blind rivets).
- The metal springs on the bottom of the housing must have low-impedance contact with the DIN rail (wide contact surface is possible).

6.2.2 WAGO DIN Rails

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

Table 45: WAGO DIN Rails

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

NOTICE

Observe the mounting distance of the DIN rail when the load is increased!

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

6.3 Spacing

A minimum distance of at least 35 mm to cable ducts and housing/frame walls must be maintained for the entire fieldbus node. Depending on the installation position the distance (D) to the power supply is 0 ... 10 mm (see chapter "Mounting" > "Installation Position").

For components that are adjacent on the DIN-rail, this distance can fall below this minimum if necessary.

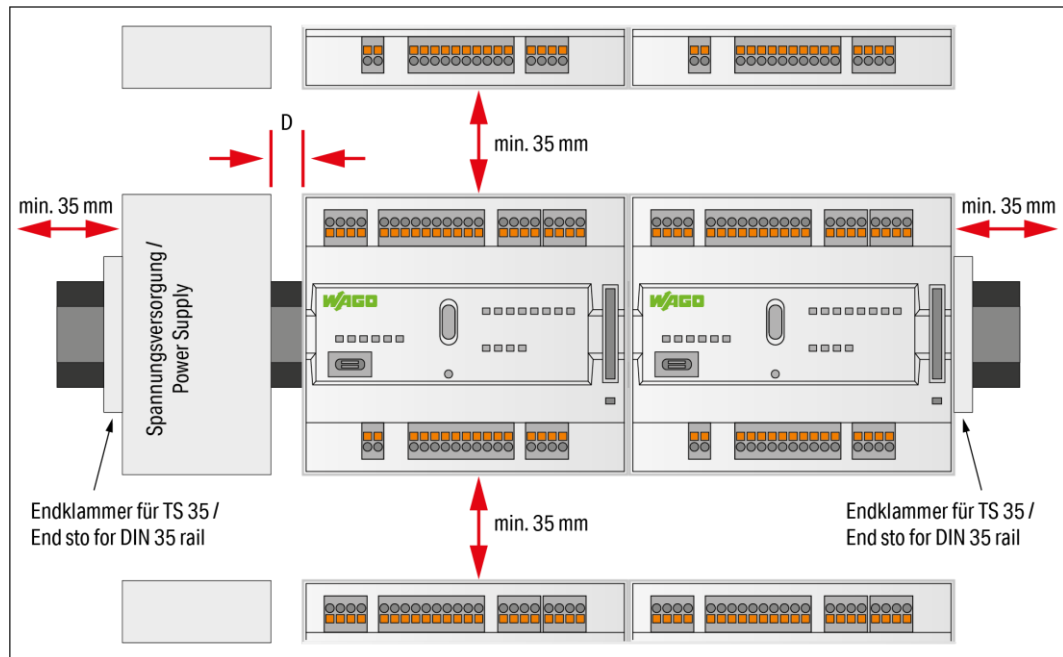


Figure 11: Spacing

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

If the installation space in the control cabinet or small installation distribution boards is limited, use angled network cables or patch cables for the X1 and X2 network connections, if necessary.

6.4 Inserting Devices



DANGER

Do not work when devices are energized!

High voltage can cause electric shock or burns.

Switch off all power to the device prior to performing any installation, repair or maintenance work.

6.4.1 Inserting the Controller

Snap the controller onto the DIN-rail.

The DIN-rail release tab automatically jumps back into the housing once the controller is locked onto the DIN-rail.

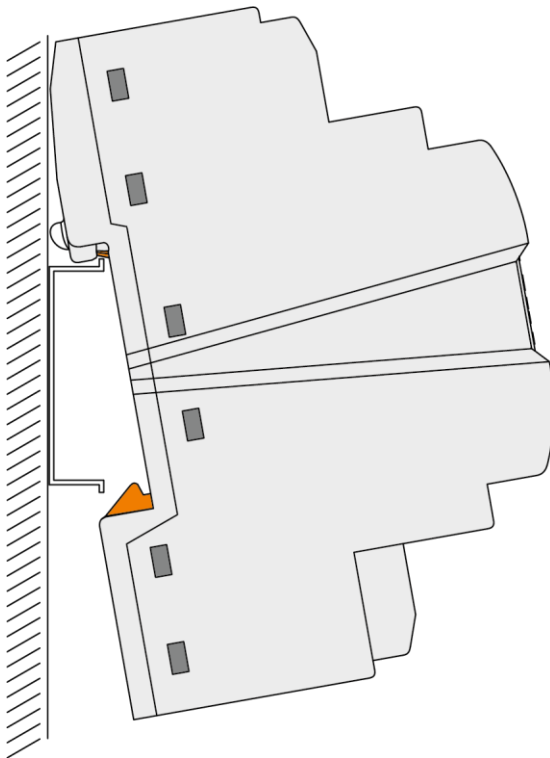


Figure 12: Insert Controller

6.4.2 WAGO *picoMAX*® Connectors

WAGO's *picoMAX*® pluggable connectors enable you to prewire devices to expedite device installation and avoid rewiring during device replacement.

WAGO *picoMAX*® connectors consist of a male header (fixed in the device) and a female connector (pluggable).

Additional information on *picoMAX*® is available in the catalog "*picoMAX*® – The Pluggable Connection System" or online at www.wago.com.

6.4.2.1 Status at delivery

When delivered, the female connectors are not plugged into the device, but included.

6.4.2.2 Removing the Female Connector

WAGO recommends using a *picoMAX*® unlocking tool (referred to in the following text as the “unlocking tool”). Further information on the unlocking tool is provided in the Section “Accessories” > “Tools”.

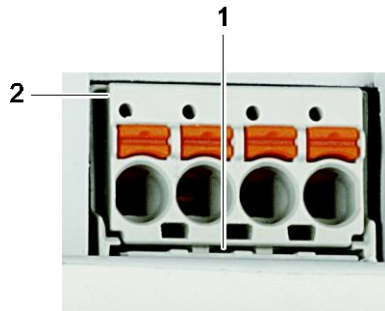


Figure 13: Removing the Female Connector without Wiring (Application Example)

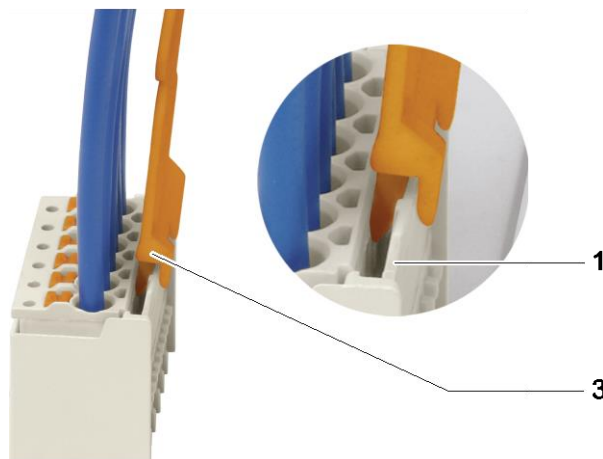


Figure 14: Removing the Female Connector with Wiring (Application Example)

Table 46: Legend for Figures “Removing the Female Connector ...”

Position	Description
1	Male locking latch
2	Protruding rim of the female connector
3	Unlocking tool

6.4.2.2.1 Removing the Female Connector without Wiring

Proceed as follows to remove the female connector with the unlocking tool:

1. Place the unlocking tool (3) onto the locking latch (1).

2. Insert the unlocking tool fully.
Wedge opens locking latches (also see the figure “Removing the female connector with wiring”).
3. Grip underneath the protruding rim of the female connector (2).
4. Pull out the female connector.

If you do not have an unlocking tool available, you can also remove the female connector with a WAGO operating tool or a screwdriver



WARNING

Do not insert the tool in the ventilation slots!

Components inside the device may be damaged if the blade of an operating tool enters the ventilation slots. This may lead to serious damage with a risk of injury caused by malfunction, overheating or electric shock!

When using a screwdriver or an actuation tool, ensure correct positioning between the locking latch and the female connector!

Proceed as follows:

1. Push the locking latch (1) away from the female connector using the screwdriver or operating tool.
2. Grip underneath the protruding rim of the female connector (2).
3. Pull out the female connector.

6.4.2.2.2 Removing the Female Connector with Wiring

Proceed as follows to remove the female connector with the unlocking tool:

1. Place the unlocking tool (3) onto the locking latch (1).
2. Insert the unlocking tool fully.
Wedge opens locking latches.
3. Pull out the unlocking tool together with the cables and the female connector.

If you do not have an unlocking tool available, you can also remove the female connector with a WAGO operating tool or a screwdriver

**WARNING****Do not insert the tool in the ventilation slots!**

Components inside the device may be damaged if the blade of an operating tool enters the ventilation slots. This may lead to serious damage with a risk of injury caused by malfunction, overheating or electric shock!

When using a screwdriver or an actuation tool, ensure correct positioning between the locking latch and the female connector!

NOTICE**Do not pull on the cables when using a screwdriver or operating tool!**

When using a screwdriver or operating tool to remove the female connector **do not** pull on the cables!

Grip underneath the protruding rim of the female connector to pull it out.

6.4.2.3 Plugging in the Female Connector**Note**

Make sure that the *picoMAX*® Female Connectors are mated properly!

Make sure that the female connector is properly mated!

Proceed as follows to plug the female connector into the corresponding male header:

1. Insert the female connector into the corresponding male header.

**Note****Ensure the correct alignment!**

Make sure that the female connector is inserted with the correct alignment: The orange push-buttons must point inward from the device.

2. Push in the female connector until the female connector snaps into position with an audible click.
3. When plugging in with wiring: Check that the female connector is seated securely by gently pulling on the wires.

7 Connecting

7.1 Earthing

The controller is grounded by the spring contacts on the underside of the product by snapping it onto the grounded DIN-rail (see figure in “Mounting” > “Insert Controller”).

7.2 Connecting Devices

The **ETHERNET interfaces** are used to connect to a LAN or to the Internet for communication with the controller. Crossover or patch cables category 5e can be used.

NOTICE

Do not use USB devices connected to earth!

USB interface shielding is not earthed directly, rather via interference-suppression capacitor. Only keyboards, mice and USB memory sticks may be connected. Do not connect devices that are earthed, e.g., printers, because they bridge the interference-suppression capacitors and thus interference immunity is reduced.

Insert **microSD** memory cards as far into the slot until they click into place. The slot can be sealed to protect the card.

To remove, press the card further down until the lock releases. The card can then be removed.

The USB service interface is designed as a USB-C socket. The interface supports USB Specification 2.0.

The controller appears on the host device (PC) as a peripheral device in device mode.

The controller uses the fixed IP address 192.168.42.42 to communicate with a PC.

For more information about the interfaces, see section “Device Description” > “Connectors” and “Technical Data”.

7.3 Connecting the Power Supply

Connect the power supply to connector X4, pin 1 (U_S+) and 2 (GND). To do this, you must also use the included 2091-1122 Female Connector.

8 Commissioning

8.1 Switching On the Controller

Before switching on the controller ensure that you

- have properly mounted the controller (see section “Mounting”),
- have connected all required data cables (see section “Connections”) to the corresponding interfaces,
- have connected the electronics and field-side power supply (see section “Connections”),
- have performed appropriate potential equalization at your machine/system and
- have performed shielding properly.

To switch on both the controller, switch on your power supply unit.

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

The runtime system CODESYS V3 is started at the same time.

Once the entire system has been successfully started, the SYS LED lights 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”).

8.2 Determining the IP Address of the Host PC

To ensure that the host PC can communicate with the controller via ETHERNET, the host PC and controller 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.
Enter the “cmd” command in the input field under **Start > Windows System > Execute** (Windows® 10) or **Start > Search programs/files** (Windows® 7).
2. Click **[OK]** button or press **[Enter]** to confirm the entry.
3. Enter the “ipconfig” command at the command prompt.
4. Press **[Enter]** to confirm the entry. The IP address, subnet mask and standard gateway, including the appropriate parameters, are displayed.

8.3 Setting an IP Address

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

Table 47: 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 (e.g., WBM or WAGO ETHERNET Settings – 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 48: Network Mask 255.255.255.0

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

8.3.1 IP Connection via USB

1. Connect the controller to your PC via the USB service interface and a suitable USB-C service cable.
2. If you are using Windows 10, go to step 4.
In Windows 7, the controller behaves like an external drive after connection. A driver for the IP connection via USB is stored on the drive.
3. Install this driver.
Communication is then possible via the IP connection via USB.
4. Call up the fixed IP address 192.168.42.42 in the browser.
The Web-Based Management of the controller opens. You can use it to make all the necessary settings on the controller.

8.3.2 Changing an IP Address using “WAGO Ethernet Settings”



Note

Note the WAGO Ethernet Settings version!

The product is compatible from WAGO Ethernet Settings version 06.15.03.02.

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

You can use a suitable USB-C service cable or the IP network for data communication.

1. Switch off the power supply to the controller.
2. Establish a suitable connection (see above) between the controller and your PC.
3. Switch on the power supply to the controller again.
4. Start the “WAGO Ethernet Settings” program.

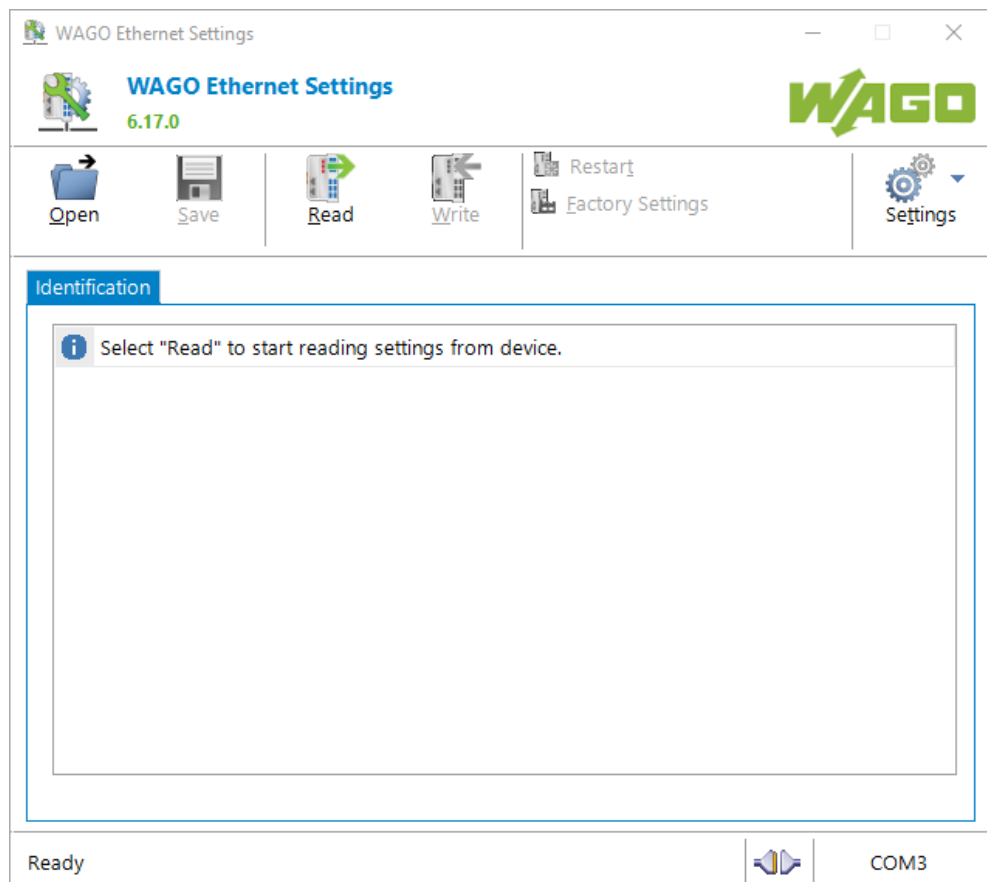


Figure 15: “WAGO Ethernet Settings” – Starting Screen (Example)

5. Click **[Read]** button 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	192.168.1.10	192.168.1.10
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	not available
Hostname		PFC200V3-46C828
Domain name	localdomain.lan	localdomain.lan

Interface X1
Interface X2
Run WBM

Interfaces
☒ Switched
☐ Separated

Figure 16: “WAGO Ethernet Settings” – “Network” Tab (Example)

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 “Input” column, enter the required IP address and, if applicable, the address of the subnet mask and of the gateway.
9. Click the **[Write]** button to apply the address in the controller. (If necessary, “WAGO Ethernet Settings” will restart your controller automatically. This action can take about 30 seconds.)
10. You can now close “WAGO Ethernet Settings”, or make other changes directly in the Web-based Management system as required. Click the **[Run WBM]** button in the right in the pane.

8.3.3 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.

8.3.4 Setting the IP Address via the WBM

You can change the IP address of the controller directly via the built-in Web-Based Management without additional tools.

1. Use a suitable network cable to connect the controller and your PC.
2. Open an internet browser on the PC.
3. Call up the WBM on the controller. To do this, enter the following in the input line of the browser: "https://<IP address>/wbm".
4. If you do not know the IP address, determine the IP address as described above.
You will then be asked to authenticate.
5. Enter the user name "user" and the corresponding password ("user" by default).
If you have not already changed the default password, you are asked to change the password now.
6. Open the "Configuration" tab.
7. In the navigation, select the "Networking" item and "TCP/IP Configuration" subitem.
8. In the "TCP/IP Configuration" group, select the "Static IP" entry in the "IP Source" selection field.
9. Enter the required IP address in the "Static IP Address" input field.
10. Enter the required subnet mask in the "Subnet Mask" input field.
11. Click the **[Submit]** button to apply the changes.
Changing the IP address interrupts the connection to the controller.
12. Establish a new connection with the new IP address.

8.3.5 Assigning an IP Address using DHCP

The controller can obtain its dynamic IP address from a server (DHCP). In contrast to fixed IP addresses, dynamically assigned addresses are not stored permanently. Therefore, a 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 conjunction with the DNS server associated with DHCP, the device can be reached using its host name. This consists of a prefix and the MAC address or part of it. The MAC address of the device can be printed on the label on the side of the device.

The following example shows the corresponding output of “Open DHCP”.

```
C:\OpenDHCPServer>
C:\OpenDHCPServer>
C:\OpenDHCPServer>OpenDHCPServer.exe -v
Open DHCP Server Version 1.75 Windows Build 1052 Starting...
Logging: All
Warning: No IP Address for DHCP Static Host 00:ff:a4:0e:ef:99 specified
Warning: No IP Address for DHCP Static Host ff:00:27:78:7b:01 specified
Warning: No IP Address for DHCP Static Host ff:00:27:78:7b:02 specified
Warning: No IP Address for DHCP Static Host ff:00:27:78:7b:03 specified
Default Lease: 36000 (sec)
Server Name: DESKTOP-67MMSRM
Detecting Static Interfaces..
Lease Status URL: http://127.0.0.1:6789
Listening On: 192.168.2.1
Network changed, re-detecting Static Interfaces..
DHCPDISCOVER for 00:30:de:46:68:98 () from interface 192.168.2.1 received
Host 00:30:de:46:68:98 (Host0030de466898) offered 192.168.2.201
Lease Status URL: http://127.0.0.1:6789
Listening On: 192.168.2.1
Network changed, re-detecting Static Interfaces..
DHCPREQUEST for 00:30:de:46:68:98 () from interface 192.168.2.1 received
Host 00:30:de:46:68:98 (Host0030de466898) allotted 192.168.2.201 for 36000 seconds
```

Figure 17: “Open DHCP”, Example Figure

In the example shown, the prefix is “Host” and the MAC ID is “00:30:de:46:68:98”.

The host name is “Host0030de466898”.

8.4 Testing the Network Connection

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

1. Open the MS DOS prompt window.
To do this, enter the command "cmd" in the input field under **Start > Execute...** > **Open:** (Windows® XP) or **Start > Search programs/files** (Windows® 7) and then click **[OK]** or press **[Enter]**.
2. In the MS DOS window, enter the command "ping" and the IP address of the controller (for example, ping 192.168.1.17) and then press **[Enter]**.

Note



Host entries in the ARP table!

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

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

```
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 18: Example of a Function Test

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

8.5 Changing Passwords



Note

Change standard passwords

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

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

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

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

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

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

1. Connect the controller to a PC via the network interfaces X1.
2. Start a terminal program on the PC.
3. Log in on the controller as user "root" with the standard password.
4. Change the password for all users with the "passwd root," "passwd admin" and "passwd user" commands.

8.6 Shutdown/Restart

Switch off the power supply to shut down the controller.

To perform a controller restart, press the Reset button as described in the Section “Triggering Reset Functions” > “Software Reset (Restart).”

Alternatively, you can switch off the controller and switch it back on again.

Note



Do not power cycle the controller after changing any parameters!

Some parameter changes require a controller restart for the changes to apply. Saving changes takes time.

Do not power cycle the controller to perform a restart, i.e., changes may be lost by shutting down the controller too soon.

Only restart the controller using the software reboot function. This ensures that all memory operations are completed correctly and completely.

8.7 Initiating Reset Functions

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

8.7.1 Warm Start Reset

All CODESYS V3 applications are reset with a warm start reset. All global data is set to its initialization values. This corresponds to the CODESYS V3 IDE "Reset warm" command.

To perform a warm start reset, set the mode selector switch to "Reset" and hold it there for two to seven seconds.

Execution of the reset is signaled by the red "RUN LED" briefly going out when the mode selector switch is released.

8.7.2 Cold Start Reset

All CODESYS V3 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 CODESYS V3 IDE "Reset Cold" command.

To perform a cold start reset, set the mode selector switch to "Reset" and hold it there for more than seven seconds.

Execution of the reset is signaled after seven seconds by the "RUN" LED going out for an extended period. You can then release the mode selector switch.

8.7.3 Software Reset

The controller is restarted on a software reset.

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

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

8.7.4 Controller Reset

NOTICE

Do not switch the controller off!

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

Note



Parameters and passwords are overwritten!

Parameters and passwords for the Linux® and WBM users of the controller are overwritten by a controller reset.

Stored boot projects are deleted, including existing web visualizations.

Subsequently installed firmware functions are not overwritten.

Software licenses are retained.

The inactive system is not changed by the reset.

If you have any questions, contact WAGO Support.

The controller is restarted after the controller reset.

Proceed as follows to reset the controller:

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

Note



Do not interrupt the reset process!

If you release the Reset button (RST) too early, then the controller restarts without performing the controller reset.

8.8 Configuration



Note

Check firmware version and update if required!

At the beginning of initial configuration check to ensure that you have the latest firmware version for the controller.

The firmware version installed on the controller is given on the WBM page "Status Information".

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 via the PC using "WAGO Ethernet Settings" (section "Configuration Using 'WAGO Ethernet Settings'").

8.8.1 Configuration via Web-Based-Management (WBM)

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

1. Connect the controller to the ETHERNET network via the ETHERNET interface X1.
2. Start a Web browser on your PC.
3. Enter “https://” followed by the controller's IP address and “/wbm-ng” in the address line of your web browser, e.g., “https://192.168.1.17/wbm-ng”. Note that the PC and the controller must be located within the same subnet (see Section “Setting an IP Address”).
If you do not know the IP address and cannot determine it, switch the controller temporarily to the pre-set address “192.168.1.17” (“Fixed IP address” mode, see Section “Commissioning” > ... > “Temporarily Setting a Fixed IP Address”).

Note



Take usage by the CODESYS program into account

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

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

WAGO

Hostname: PFC200V3-42E739

Description: WAGO 750-8216 PFC200 G2
2ETH RS CAN DPS Tele T

Username

Password

Login

Figure 19: Entering Authentication

4. Enter the username and password.
5. Click the **[Login]** button.

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

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

8.8.1.1 WBM User Administration

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

Note



Change passwords

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

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

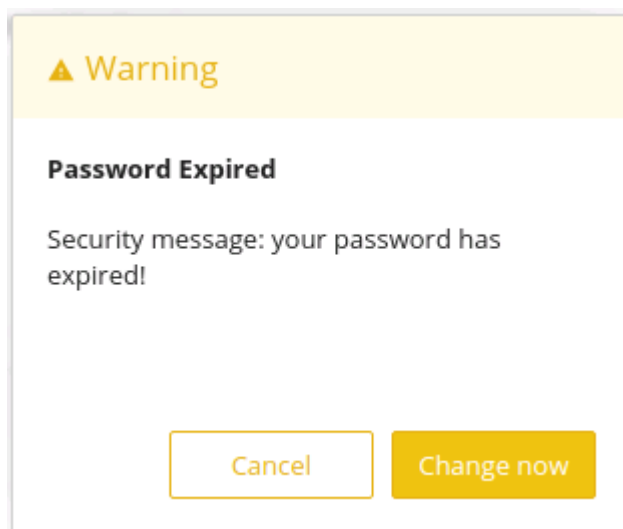


Figure 20: Password Reminder

Table 49: User Settings in the Default State

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

Note



General Rights of WBM Users

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

User administration for controller applications is configured separately.

Access rights for the WBM pages are shown in the table below.

The “root” user has the same rights as the “admin” user and is therefore not listed separately.

Table 50: Access Rights for WBM Pages

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

Table 50: Access Rights for WBM Pages

Tab/Navigation	WBM Page Title	User
Connection 1	Configuration	admin
Connection 2	Configuration	admin
SNMP		
General Configuration	Configuration of general SNMP parameters	admin
SNMP v1/v2c	Configuration of SNMP v1/v2c parameters	admin
SNMP v3	Configuration of SNMP v3 Users	admin
Commissioning	Commissioning Settings	admin
Docker	Docker Settings	admin
Users	WBM User Configuration	user
Fieldbus		
OPC UA	OPC UA Configuration	admin
BACnet		
Status	BACnet Status	admin
Configuration	BACnet Configuration	admin
Data Link	BACnet Data Link	admin
Storage Location	BACnet Storage Location	admin
Security		
OpenVPN / IPsec	OpenVPN / IPsec Configuration	admin
Firewall		
General Configuration	General Firewall Configuration	admin
Interface Configuration	Interface Configuration	admin
MAC Address Filter	Configuration of MAC Address Filter	admin
User Filter	Configuration of User Filter	admin
Certificates	Certificates	admin
Boot Mode	Boot mode configuration	admin
TLS	Security Settings	admin
Integrity	Advanced Intrusion Detection Environment (AIDE)	admin
WAGO Device Access	WAGO Device Access	admin
Diagnostic		
Log Message	Log Message Viewer	user
Download	Download	admin
Network Capture	Network Capture	admin

8.8.1.2 General Information about the Page

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

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

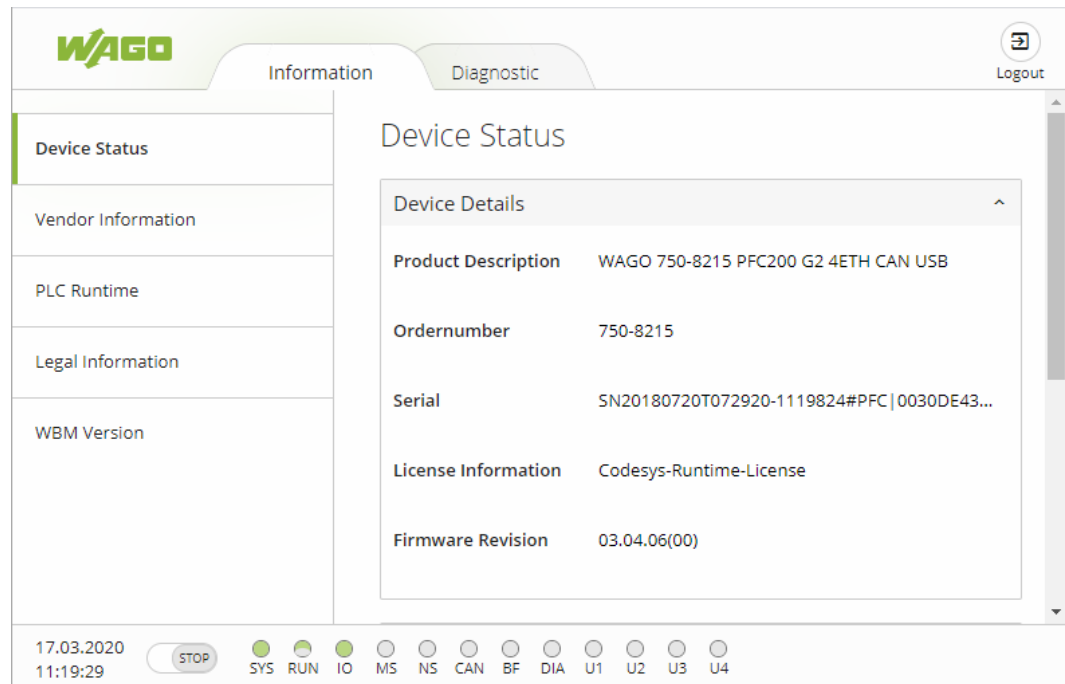


Figure 21: WBM Browser Window (Example)

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

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

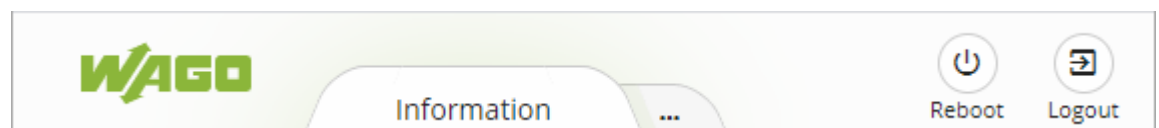


Figure 22: WBM Header with Tabs that Cannot be Displayed (Example)

The navigation tree is shown on the left of the browser window. The content of the navigation tree depends on the selected tab.

You can use this navigation tree to go to the individual pages and, where provided, subpages included in these pages.

The current device status is displayed in the status bar.

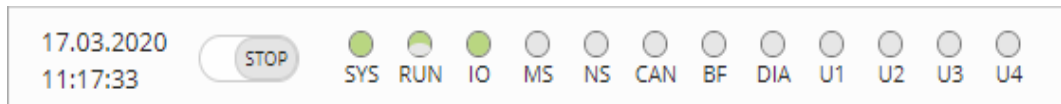


Figure 23: WBM Status Bar (Example)

- Date and Time - Local date and local time and on the device
- Setting of the mode selector switch
- LED status of the Device:
All LEDs are graphically represented and are labeled with their particular designation (e.g., SYS, RUN, ...). The following colors are possible:
 - gray: LED is off.
 - full color (green, red, yellow, orange): The LED is activated in the particular color.
 - half color:
The LED is flashing in the corresponding color. The other half of the surface is then either gray or also colored. The latter case indicates that the LED is flashing sequentially in different colors.

A tooltip containing more detailed information opens as long as the cursor is positioned over an LED. The text that is displayed also contains the message that put the LED into its current status. The time of the message is also shown.

The states displayed in the WBM will not always correspond at the precise time to those on the controller. Data has a runtime during transmission and can only be queried at a certain interval. The time period between two queries is 30 seconds.



Note

Do not power cycle the controller after changing any parameters!

Some parameter changes require a controller restart for the changes to apply. Saving changes takes time.

Do not power cycle the controller to perform a restart, i.e., changes may be lost by shutting down the controller too soon.

Only restart the controller using the software reboot function. This ensures that all memory operations are completed correctly and completely.

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

8.8.2 Configuration 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 06.15.01 dated 2021-02-08 or newer of “WAGO Ethernet Settings”!

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

You can use a suitable USB-C service cable or the IP network for data communication.

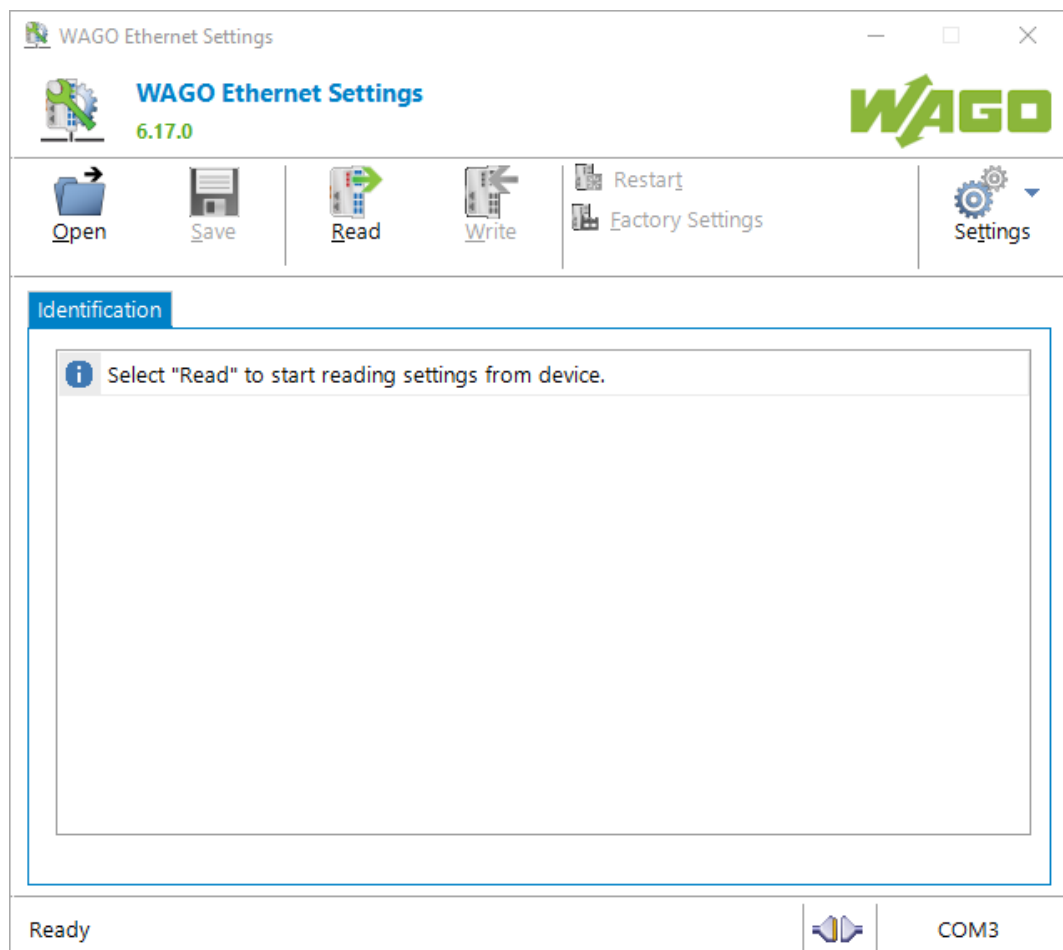


Figure 24: “WAGO Ethernet Settings” – Start Screen (Example)

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

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

Communication Settings

Connection

Serial Ports (COM, USB, Bluetooth,...)

Settings

Port:

COM3: Intel(R) Active Management Technology

Baud rate: 19200 Parity: Even Data bits: 8 Stop bits: 1

Timeout [s]: 15 Restart-Timeout [s]: 10

Default Apply Cancel

Figure 25: "WAGO Ethernet Settings" – Communication Link (Example)

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

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

8.8.2.1 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.

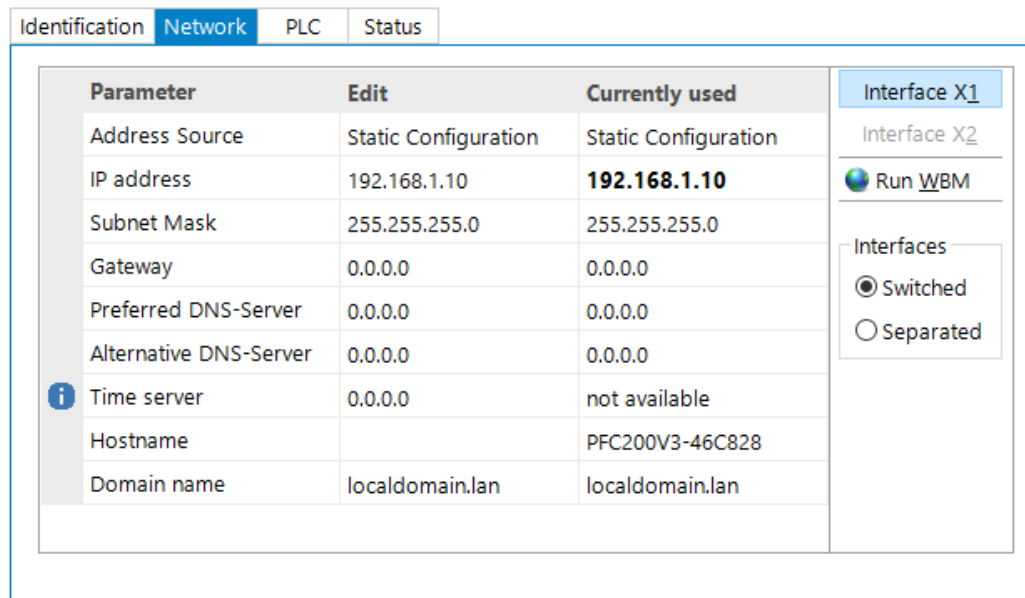
Identification	Network	PLC	Status
Item Number	750-8210		
Description	WAGO 750-8210 PFC200 G2 4ETH		
FW Version	04.01.09(00)		
HW Version	01		
FWL Version	2021.10.0w04.00.00 IDX=14		
Serial Number	375UN31564010260372744+9999999999999999		
MAC address	0030DE46C828		
IP address	192.168.1.10 (Static Configuration)		
Runtime system	CODESYS V3		

Figure 26: “WAGO Ethernet Settings” – Identification Tab (Example)

8.8.2.2 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	192.168.1.10	192.168.1.10
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	not available
Hostname		PFC200V3-46C828
Domain name	localdomain.lan	localdomain.lan

Figure 27: “WAGO Ethernet Settings” – Network Tab (Example)

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, the host name is composed of the string “CC100” and the last three bytes of the

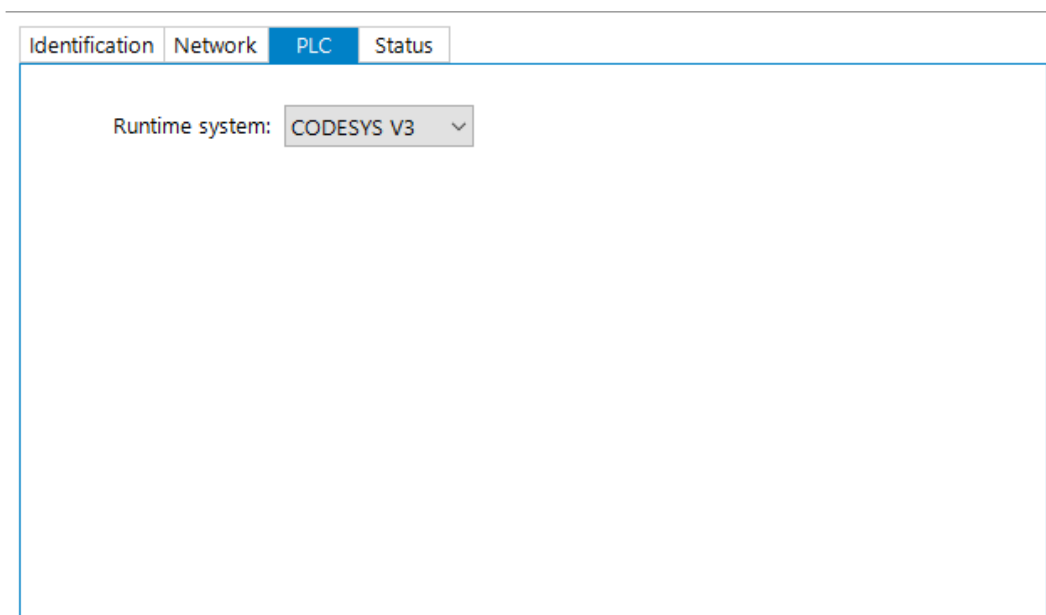
MAC address.

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

Domain name

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

8.8.2.3 PLC Tab



The screenshot displays the 'WAGO Ethernet Settings' window with the 'PLC' tab selected. The 'Runtime system:' dropdown menu is set to 'CODESYS V3'.

Figure 28: “WAGO Ethernet Settings” – Protocol Tab (Example)

Here you can select the runtime system.

8.8.2.4 Status Tab

Identification Network PLC **Status**

Status

- ☐ Field bus active
- ☐ Write access enabled
- ☐ Monitor-Mode enabled
- ☐ Control-Mode enabled
- ☐ Factory test mode enabled

Blink code

Error code: 0

Argument: 0

No Error

Figure 29: "WAGO Ethernet Settings" – Status Tab (Example)

General information about the controller status is displayed here.

9 Run-time System CODESYS V3

9.1 General Notes



Note

Additional Information

Information on the installation, startup and programming is provided in the CODESYS V3 documentation.

9.2 CODESYS V3 Priorities

A list of priorities implemented for the controller is provided below as supplementary information to the CODESYS V3 documentation.

Table 51: CODESYS V3 Priorities

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

9.3 Memory Spaces under CODESYS V3

The memory spaces in the controller under CODESYS V3 have the following sizes:

- Program memory: 32 Mbytes
- Data memory: 128 Mbytes
- Input data: 64 kbytes
- Output data: 64 kbytes
- Retain/Persistent: 128 kbytes
- Function block limitation: $12 * 4096 \text{ bytes} = 48 \text{ kbytes}$

9.3.1 Program and Data Memory

The program memory (also code memory) has a maximum size of 32 MB.

The data memory has a maximum size of 128 MB.

Both areas are separate from each other and are requested when downloading to the system depending on the scope of the program. If the size limit is exceeded, it is displayed as an error.

9.3.2 Function Block Limitation

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

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

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

9.3.3 Remanent Memory

A total of 128 kbytes of remanent memory is available for the IEC-61131 application.

The remanent area is divided into the retain area and the persistence area. The areas are automatically distributed by CODESYS V3.

9.3.4 File Access from the IEC Application

Access to files via the IEC application is restricted to the following directories:

- /home/codesys
- /media/sd
- /tmp

9.3.5 Changing Network Settings from the IEC Application

To change network settings from an IEC application or via a fieldbus (e.g., PROFINET DCP), the “IP Source” parameter must be set to “external” (WBM “TCP/IP Configuration” page – “Bridge Interfaces” group).

The IEC application changes the network settings, for example, by enabling the “Adjust operating system settings” option in CODESYS (double-click the “ETHERNET (ETHERNET)” element in the device tree > “General” tab > “Adjust operating system settings” option).

9.3.6 EtherCAT

EtherCAT connection is possible via the CODESYS V3 functionality and the CODESYS V3 libraries.

To use the EtherCAT master function, the network interfaces must be switched from “switched” to “separated” (WBM “ETHERNET Configuration” page – “Bridge Configuration” group) and the controller or at least the runtime restarted so that the MAC addresses are assigned correctly.

To configure the EtherCAT master added to the project, the required AC adapter is selected in CODESYS (double-click the “EtherCAT_Master” element in the device tree > “General” tab > “Source address MAC” > **[Select]**).

9.4 Process Image

9.4.1 Analog Inputs

The analog inputs AI1 and AI2 are represented per channel via the WORD data type (16 bit).

Table 52: Process Image – Analog Inputs

Channel	Pin	Data Type	Measured Value	Value Range		
				Hex.	Dec.	Bin.
AI1	X14.1	WORD	< 0 V	0x0000	0	0000.0000. 0000.0000
			0 ... 10 V	0x0000 ... 0x7FF8	0 ... 32760	0000.0000. 0000.0000 ... 0111.1111. 1111.1000
AI2	X14.3		> 10 V	0x7FFB	32763	0111.1111. 1111.1011

9.4.2 Analog outputs

The analog outputs AO1 and AO2 are represented per channel via the WORD data type (16 bit).

Table 53: Process Image – Analog Outputs

Channel	Pin	Data Type	Measured Value	Value Range		
				Hex.	Dec.	Bin.
AO1	X6.1	WORD	0 ... 10 V	0x0000 ... 0x7FFF	0 ... 32767	0000.0000.
AO2	X6.3					0000.0000 ... 0111.1111. 1111.1111

9.4.3 Analog Temperature Inputs

The analog temperature sensor inputs PT1+ / PT1– and PT2+ / PT2– are represented at a resolution of 1 digit per 0.1 °C via the INT data type (16 bit).

Table 54: Process Image – Analog Temperature Inputs

Channel	Pin	Data Type	Measured Value	Value Range		
				Hex.	Dec.	Bin.
PT1+ / PT1–	X13.1 / X13.2	INT	< –60 °C	0x8001	–32767	1.000.000. 000.000.000
			–60 °C ... 350 °C	0xFDA8* ... 0x0DAC	–600 ... 3500	1111.1101. 1010.1000* ... 0000.1101. 1010.1100
PT2+ / PT2–	X13.3 / X13.4		> 350 °C	0x0DAC	3500	0000.1101. 1010.1100

*Temperature values below 0 °C are represented in two's complement binary and hexadecimal.

9.4.4 Digital Inputs

The digital inputs DI1 ... DI8 are represented per channel via the BOOL data type. In addition, the digital inputs are represented via the BYTE data type.

Table 55: Process Image – Digital Inputs

Table 53: Process Image – Digital Inputs						
Channel	Pin	Data Type	Measured Value	Value Range		
				Hex.	Dec.	Bin.
DI [1 ... 8]	X12	BYTE	0 / +24 V DC	0x00 ... 0xFF	0 ... 255	0000.0000 ... 1111.1111
DI1	X12.3	BOOL		–	–	TRUE / FALSE
DI2	X12.4					
DI3	X12.5					
DI4	X12.6					
DI5	X12.7					
DI6	X12.8					
DI7	X12.9					
DI8	X12.10					

9.4.5 Digital Outputs

The digital outputs DO1 ... DO4 are represented per channel via the BOOL data type. In addition, the digital outputs are represented via the BYTE data type.

Table 56: Process Image – Digital Outputs

Chan- nel	Pin	Data Type	Mea- sured Value	Value Range		
				Hex.	Dec.	Bin.
DI [1 ... 8]	X5	BYTE	0 / +24 V DC	0x00 ... 0x0F	0 ... 15	0000.0000 ... 0000.1111
DO1	X5.3	BOOL		–	–	TRUE / FALSE
DO2	X5.5					
DO3	X5.7					
DO4	X5.9					

10 CANopen Master and Slave

Based on IEC 61131-3 programming, data processing occurs on site in the controller. The process results can be output directly to the actuators, or transmitted via the bus.

Process data is exchanged with PDOs and SDOs. The controller supports 512 TX PDOs and 512 RX PDOs and 128 SDOs to send process data via the CANopen fieldbus.

In the local process image, a range of 4096 bytes serves as each input and output range for data exchange via the CANopen interface. Direct access to the I/O modules via the fieldbus is not provided.

All entries of the process image can be mapped as required to the RX PDOs and TX PDOs. The entire input and output data area can be read and written via SDOs.

After initialization, CANopen communication runs independently of the IEC application.

When used as a CANopen slave, the baud rate and the bus address can be changed according to the CANopen LSS protocol.

10.1 Object Directory

All CANopen communication and process data objects are compiled in the object directory.

The following table gives a general overview of the CANopen definition:

Table 57: Overview of Addresses in the Object Directory

Index Range	Use
0000	Not used
0001-009F	Data types
00A0-0FFF	Reserved (addresses used for other services)
1000-1FFF	Communication profile
2000-5FFF	Vendor-specific range
6000-9FFF	Up to eight standardized device profiles
A000-AFFF	Process images from IEC 61131 devices
B000-BFFF	Process images from CANopen gateways acc. CiA 302-7
C000-FFFF	Reserved

The relevant objects available on the controller are described below.

10.2 Communications Profile

0x1000 Device Type

The stack responds on the bus as the DS-405 device (IEC 61131-3 programmable device), regardless of being configured as the master or slave. As direct access to the I/O modules via the bus is prohibited, the bits for information about inputs and outputs are 0.

Entry 0x000191 = DS 405 for master and slave

0x1001 Error Register

This entry contains an 8-bit item of information about the error status. At present, bit 4 is used specifically for communication and bit 5 for the device profile. Bit 0 is set for each error.

0x1003 Pre-defined Error Field

This entry contains the list of accumulated errors which were signaled in error register 0x1001. Sub-index 0 contains the number of entries. If a new error occurs, it is added to sub-index 1 and all existing errors are moved down one sub-index. A maximum of 20 error entries is supported. If more than 20 errors occur, the error at sub-index 20 is overwritten. By writing a "0" into sub-index 0, the complete error memory is deleted.

Standard values: 0 in all entries

0x1005 COB ID Sync

This object defines the COB ID for the synchronization message.

Default: 0x80

0x1006 Communication Cycle Period

The duration of the synchronization cycle given in μs , or 0 for cyclic synchronization. Internal resolution is 1 ms. If this value is 0, SYNC monitoring does not occur.

Default: 0

0x1008 Manufacturer Device Name

This object specifies the device name.

Entry: Item No. for the PFC200, e.g., "750-8206"

0x1009 Manufacturer Hardware Version

Entry: "V 1.0" or higher

0x100A Manufacturer Software Version

Entry: "04.02.05(00)" or higher

0x100C Node Guarding Time

The object specifies the "Guarding Time" in milliseconds. An NMT master requests the state of the NMT slave in a cyclical manner. The time between two requests is the "Guarding Time."

Default: 0 (Node guarding disabled)

0x100D Life Time Factor

The "Life Time Factor" is part of the node guarding protocol. The NMT slave checks whether it was queried within the node lifetime (guarding time multiplied by the lifetime factor). If not, the slave must assume that the NMT master is no longer in normal operation; it then initiates a "life guarding event".

Default: 0 (Node guarding off)

0x1012h COB-ID Time Stamp Object

The time stamp object enables every device's clock on the bus to be synchronized. The ID for this object is indicated here. Although the synchronization signal is not evaluated by the runtime, it may be used with library functions.

Default: 0x100 (Time Stamp Consumer)

0x1014h Emergency COB ID

An emergency message is transmitted in the event of CANopen device errors. The ID for this object is indicated here.

Default: 0x80 + Device ID

0x1015h Emergency Inhibit Time

This object specifies the minimum time that must elapse before another emergency object is sent. An entry equal to zero disables delayed sending. One time unit amounts to 100µs.

Default: 0

0x1016h Consumer Heartbeat Time

This entry can be used for monitoring of other devices on the bus. A check is made to determine whether each module defined in this object has generated a heartbeat within the set time. If the set time has been exceeded, a heartbeat event is triggered. The "Heartbeat Time" is entered in milliseconds. If the time is 0, monitoring is deactivated. The number of devices to be monitored is entered in index 0, the heartbeat time is entered in ms in the bottom 16 bits and the ID of the bus device in the 8 bits above that.

Default:

Index 0: 0 (currently still 127 = Number of possible entries)

All other entries are 0 (this function is not yet supported by the CAN master in Firmware 1.0).

0x1017h Producer Heartbeat Time

This object defines the time (in milliseconds) between two transmitted heartbeat messages. No heartbeat is sent if the time is set to 0.

Default: 0

0x1018h Identity

This object specifies the device being used. The manufacturer ID contains a unique number for each vendor. WAGO has been assigned an ID of 33.

The product code contains the device identifier.

The Rev. No. contains a specific CANopen behavior. The Major Rev. No. contains the CANopen functionality. If the functionality is changed, the Major Rev. No. is increased. You can use the Minor Rev. No. to distinguish between different versions with the same CANopen behavior.

The number is independent of the firmware revision.
When used as a CANopen slave with CODESYS 3.5, the vendor ID, product code and revision number can be freely defined in the slave configuration.

Sub-index 0 No. of entries:	4
Sub-index 1 vendor ID:	33
Sub-index 2 product_code:	e.g., 8216 for 750-8216
Sub-index 3 revision_number:	0x00010003 or higher
Sub-index 4 serial_number:	corresponds to the last 4 bytes of the MAC address.

0x1200, 0x1201 Server SDO Parameter Channels

The communication parameters for an SDO as the server are entered here. Two server SDO channels are supported.

0x1280 ... 0x128E Client SDO Parameter Channels

The communication parameters for an SDO transfer as the client are entered here. 16 client SDO channels are supported.

0x1029h Error Behavior

This object defines how the slave responds in the event of an error.

Sub-index 0 No. of entries: 1

Sub-Index 1 Communication Error:

- | | |
|---|---|
| 1 | No change (Standard) |
| 0 | Change from operational to preoperational |
| 2 | Change to stop |

0x1F51 Program Control

The status of the PLC can be read out using this object. Writing is prohibited.

Entries: 0 = Stop 1 = Run 2 = Reset 3 = Clear

10.2.1 Master Configuration

These objects are only available at the bus end when the master has been configured.

0x102A NMT Inhibit Time

This object indicates the minimum time that must elapse before another NMT telegram is sent. An entry equal to zero deactivates delayed sending. One unit of time is 100 µs.

Default: 0

0x1F80 NMT Start-up

This object contains the configuration bits for the master status. If automatic startup is deactivated, the master can be started by writing of 0x1F to this object.

0x1F81 ... 0x1F8A Slave Configuration

The configured slaves are entered in these lists. All of the entries are checked when the master is started and transferred to the slaves.

0x1F81 NMT Slave-Assignment

Subindex 0: 128 = Number of possible entries

Subindex 1 ... 128: Bit 0: Slave present

Bit 2: Slave required for start

Bit 3: Slave reset performed on start

Bit 8 ... 15: Guard Retry Factor

Bit 16 ... 31: Guard Time

Subindex 128: Total network (write only)

0x1F82 Request-NMT

Sub-Index 0: 127 = Number of possible entries

Sub-Index = Master Node ID NMT state of the master

0x1F84 Device Type Identification

Sub-Index 0: 127 = Number of possible entries

Sub-Index 1 ... 127: Slave device type

0x1F85 Vendor Identification

Sub-Index 0: 127 = Number of possible entries

Sub-Index 1 ... 127: Slave device type (not used by default)

0x1F86 Product Code

Sub-Index 0: 127 = Number of possible entries

Sub-Index 1 ... 127: Slave device type (not used by default)

0x1F87 Revision number

Sub-Index 0: 127 = Number of possible entries

Sub-Index 1 ... 127: Slave device type (not used by default)

0x1F88 Serial Number

Sub-Index 0: 127 = Number of possible entries

Sub-Index 1 ... 127: Slave device type (not used by default)

0x1F89 Boot Time

Time in ms between the start of slaves and operational readiness of all slaves.

Default: 0 = deactivated

0x1F8A Restore Configuration

Sub-Index 0: 127 = Number of possible entries

Sub-Index 1 ... 127: Bit 0 = 1 Send restore configuration to slave on start

10.3 Data Exchange

Process data exchange occurs via the communication objects with the CANopen fieldbus controller.

Each object consists of a CAN telegram with a maximum of 8 bytes process data and a COB (Communication Object Identifier) ID that is unique within the network.

These communication objects transmit data, trigger events, signal error statuses, etc.

The parameters required for the communication objects, as well as CANopen device parameters and data are stored in an object directory.

10.3.1 Controller Communication Objects

The PFC200 supports the following communication objects:

512 Tx-PDOs for process data exchange from input data of the fieldbus node

512 Rx-PDOs for process data exchange from output data of the fieldbus node

Synchronization objects (SYNC) for network synchronization

Emergency objects (EMCY)

Network management objects

- Module Control Protocols
- Error Control Protocols
- Boot-up Protocol

10.3.2 Fieldbus-Specific Addressing

The CODESYS variable for the CAN bus are mapped to an object directory after configuring the CAN interface as a master or slave (initialization). A CANopen fieldbus device uses the 16-bit indices and 8-bit sub-indices of the object directory to address data via PDOs or SDOs and to access the data. The position of the data in the process image is therefore not directly significant for the CANopen user at the fieldbus end.

The variables entered into the object directory are distinguished by data type (Integer8, Unsigned8, Boolean, Integer16, etc.) and by input/output. Access via PDOs can be either for reading or writing.

As CANopen does not transfer data by bits, the variable data is combined from a Boolean data type to bytes and assigned to the corresponding index; Boolean input variable data is assigned to index 0xA080, Boolean output variable data to index 0xA500.

Variable data that has a data width of 1 byte or more is assigned to the corresponding indices in a similar manner.

Note



Observe the direction of data flow!

The IEC 61131-3 input variables are defined from the perspective of the CAN bus. These are output variables from the perspective of the PFC. Accordingly, the IEC 61131-3 output variables are input variables for the PFC.

This table provides an overview of the indices of "IEC 61131-3" variables.

Table 58: Indexing of "IEC 61131-3" Variable Data in the Object Directory

Data Type	IEC 61131-3 Output Variables	IEC 61131-3 Input Variables
	Index	
Integer8	0xA000	0xA480
Unsigned8	0xA040	0xA4C0
Boolean	0xA080	0xA500
Integer16	0xA0C0	0xA540
Unsigned16	0xA100	0xA580
Integer24	0xA140	0xA5C0
Unsigned24	0xA180	0xA600
Integer32	0xA1C0	0xA640
Unsigned32	0xA200	0xA680
Float32	0xA240	0xA6C0
Unsigned40	0xA280	0xA700
Integer40	0xA2C0	0xA740
Unsigned48	0xA300	0xA780
Integer48	0xA340	0xA7C0
Unsigned56	0xA380	0xA800
Integer56	0xA3C0	0xA840
Integer64	0xA400	0xA880
Unsigned64	0xA440	0xA8C0

Using the associated indices for data types with a data width of 1 byte (Integer8, Unsigned8 and Boolean), read-only byte-by-byte access is possible from the fieldbus to data in the controller memory.

The sub-index is utilized to select a specific byte.

In contrast, when the indices for larger data blocks are used, several bytes can be accessed simultaneously.

For example, the described PFC output variable data can be accessed in a word-by-word manner using the index for Integer16 (0xA0C0) or for Unsigned16 (0xA100), three bytes can be accessed using index 0xA140 for Integer24, etc.

Example:

The first three bytes of the PFC output data for the data type integer or unsigned are accessed from the fieldbus:

Table 59: Fieldbus Access to PFC Output Data

Access	PFC Output Data	Reading with Index (Integer / Unsigned)	Sub-Index
By byte (with Integer8 / Unsigned8)	Byte 6000	(0xA000 / 0xA040)	1
	Byte 6001	(0xA000 / 0xA040)	2
	Byte 6002	(0xA000 / 0xA040)	3
By word (with Integer16 / Unsigned16)	Word 3000 (Byte 6000/6001)	(0xA0C0 / 0xA100)	1
	Word 3001 (Byte 6002/6003)	(0xA0C0 / 0xA100)	2
3 bytes (with Integer24 / Unsigned24)	Bytes 6000 ... 6002	(0xA140 / 0xA180)	1

The following tables give an overview of addressing data with different data widths.

In this case, the corresponding indexing is assigned to the memory space for fieldbus variables (byte 6000 to byte 9999) as a function of the data width.

The indexing indicated in the tables continues up to the respective maximum index and sub-index.

Note



Observe the direction of data flow!

The PFC output variables are defined from the perspective of the controller; from the perspective of the CAN fieldbus these are input variables. Accordingly, the PFC input variables for IEC 61131-3 access are output variables for the fieldbus.

Thus: IEC 61131-3 input variable = PFC output variable

PFC input variable = IEC 61131-3 input variable.

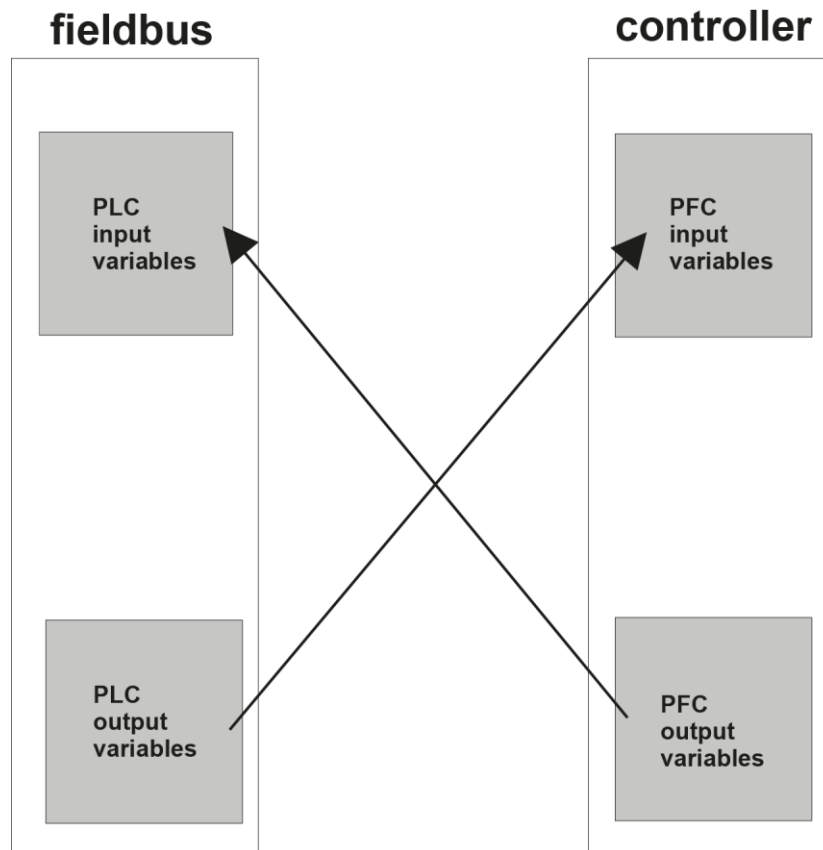


Figure 30: Correlation Between "IEC 61131-3" Variables and PFC Variables

10.3.3 Examples for the Definition of PFC Fieldbus Variables

The examples below show the allocation of several definitions for PFC variables with different data types to the associated object directory entries.

10.3.3.1 CODESYS Access to PFC Variables

Table 60: Examples for CODESYS Access to PFC Variables

Data Type of PFC Variables	PFC Input Variables		PFC Output Variables	
	Definition based on IEC 61131-3	Index/sub-index	Definition based on IEC 61131-3	Index/sub-index
Unsigned8	InByte0 AT %IB6000: BYTE;	0xA4C0/1	OutByte0 AT %QB6000: BYTE;	0xA040 /1
	InByte0 AT %IB6001: BYTE;	0xA4C0/2	OutByte0 AT %QB6001: BYTE;	0xA040 /2
Integer16	InInt0 AT %IW3000: INT;	0xA540 /1	OutInt0 AT %QW3000: INT;	0xA0C0/1
	InInt1 AT %IW3001: INT;	0xA540 /2	OutInt1 AT %QW3001: INT;	0xA0C0/2
Unsigned16	InWord0 AT %IW3000: WORD;	0xA580 /1	OutWord0 AT %QW3000: WORD;	0xA100 /1
	InWord0 AT %IW3001: WORD;	0xA580 /2	OutWord0 AT %QW3001: WORD;	0xA100 /2
Unsigned32	InDWord0 AT %ID1500: DWORD;	0xA680 /1	OutDWord0 AT %QD1500: DWORD;	0xA200 /1
	InDWord0 AT %ID1501: DWORD;	0xA680 /2	OutDWord0 AT %QD1501: DWORD;	0xA200 /2

10.3.3.2 Maximum Indices

The maximum indices and sub-indices are yielded from the memory size of the fieldbus controller at 4096 bytes and the corresponding data width for the data types.

The table below provides an overview of the maximum indices and sub-indices of the IEC 61131-3 variables.

Table 61: Maximum Indices and Sub-Indices for "IEC 61131-3" Variables

Data Type	IEC 61131-3 Input Variables		IEC 61131-3 Output Variables	
	Max. index	Max. sub-index	Max. index	Max. sub-index
Integer8	0xA00F	0xFF	0xA487	0xFF
Unsigned8	0xA04F	0xFF	0xA4C7	0xFF
Boolean	0xA08F	0xFF	0xA507	0xFF
Integer16	0xA0C7	0xFF	0xA543	0xFF
Unsigned16	0xA107	0xFF	0xA583	0xFF
Integer24	0xA145	0x55	0xA5C0	0x55
Unsigned24	0xA185	0x55	0xA600	0x55
Integer32	0xA1C3	0xFF	0xA643	0xFF
Unsigned32	0xA203	0xFF	0xA683	0xFF
Float32	0xA243	0xFF	0xA6C3	0xFF
Unsigned40	0xA283	0x33	0xA703	0x33
Integer40	0xA2C3	0x33	0xA743	0x33
Unsigned48	0xA302	0xAA	0xA780	0xAA
Integer48	0xA342	0xAA	0xA7C0	0xAA
Unsigned56	0xA382	0x49	0xA802	0x49
Integer56	0xA3C2	0x49	0xA842	0x49
Integer64	0xA401	0xFF	0xA880	0xFF
Unsigned64	0xA441	0xFF	0xA8C0	0xFF

Example:

514 bytes of output variables are addressed by word by the data type Unsigned16.

Addressing of 257 data words then occurs with:

- Index 0xA580, sub-index 1 to 255
- Index 0xA581, sub-index 1 and 2.

Table 62: Example of "IEC 61131-3" Output Variables

Index	Sub-Index	Contents	Description
0xA580	1	D1 ^{*)}	1 st output variable block
	2	D2 ^{*)}	2 nd output variable block

	255	D255 ^{*)}	255 th output variable block
0xA581	1	D256 ^{*)}	256 th output variable block
	2	D257 ^{*)}	257 th output variable block

^{*)} D1 = Data word output variable 1, D255 = Data word output variable 255, etc.

10.3.4 Using the CANopen Slave (Device) under CODESYS V3

The CODESYS 3.5 slave configurator uses other object addresses for the process data than defined in the CANopen CiA 405 standard for IEC 61131 devices. Therefore, when operating as a CODESYS V3 slave, these CODESYS V3 object numbers are used:

0x3000 .. 0x31FF	Receive process data (master => slave)
0x3800 .. 0x39FF	Send process data (slave => master)
0x5000 .. 0x507F	SDO read/write access
0x5800 .. 0x587F	SDO read access

A more detailed description on how to use the CANopen interface is provided in the CODESYS V3 online manual. The WAGO-specific functions can be used via the WagoAppCanOpen and WagoAppCanLayer2 libraries.

10.3.5 Use as a CAN Layer 2 Device

As an alternative to the CANopen master or slave function, a pure Layer2 stack is also available on the Controller. This can be used when no CANopen functions are required. It offers higher data throughput with a lower CPU load.

It is possible to set 127 receive filters with a total buffer of 127 telegrams or to use an unfiltered receive buffer of 255 telegrams.

The WAGO CanLayer2 device is selected on CAN for use with CODESYS V3. This functionality is used via the WagoAppCanLayer2 library.

11 Diagnostics

11.1 Operating and Status Messages

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

11.1.1 "SYS" LED

11.1.1.1 SYS LED

Table 63: Diagnostics via SYS LED

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

11.1.1.2 RUN LED

Table 64: 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	---

Table 64: RUN LED Diagnostics

Status	Explanation	Remedy
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.

11.1.1.3 CAN LED

The CAN LED indicates following diagnostics:

Table 65: Diagnostics CAN LED

Status	Explanation	Solution
Off	The CAN interface has not been configured	---
Alternating red 50 ms / green 50 ms	Configuration in progress	---
Alternating red 200 ms / green 200 ms	Configuration invalid	Check the configuration in the CODESYS Configurator.
Green 200 ms / off 800 ms	The CANopen interface has the status "Stop".	---
Green 200 ms / off 200 ms	The CANopen interface has the status "Preoperational".	---
Green	The CANopen interface has the status "Operational".	---
Red	The CANopen interface has the status "Bus Off" (short-circuit or other major fault).	Check the bus connections and the baud rate.
Error in the status "Preoperational"		
1* red flashing / 2 * green flashing	"Bus Warning Level" exceeded.	Check the wiring for the CAN bus.
2* red flashing / 2 * green flashing	"Guarding Error", slave incorrectly configured or not available.	Check the slaves and the configuration.
3* red flashing / 2 * green flashing	"Sync Error"	Change the time interval for the synchronization message.
Error in the status "Operational"		
1* red flashing / green 800 ms on	"Bus Warning Level" exceeded.	Check the wiring for the CAN bus.
2* red flashing / green 800 ms on	"Guarding Error"	Check the slaves and the configuration.
3* red flashing / green 800 ms on	"Sync Error"	Change the time interval for the synchronization message.

11.1.2 Network Connection LED

11.1.2.1 "LNK ACT" LED

The "LNK ACT" LED indicates following diagnostics:

Table 66: "LNK ACT" LED Diagnostics

Status	Explanation	Remedy
Off	No network communication via port	Check network connections and network settings.
Green	Connection to the physical network available	---
Green flashing	Network communication via port	

11.1.3 Memory Card Slot LED

The memory card slot LED indicates following diagnostics:

Table 67: Diagnostics via Memory Card Slot LED

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

12 Service

12.1 Inserting and Removing the Memory Card

12.1.1 Inserting the Memory Card

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

12.1.2 Removing the Memory Card

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

12.2 Firmware Changes

NOTICE

Do not switch the controller off!

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

Note



Obtain documentation appropriate for the firmware target version!

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

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

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

Note



Note the firmware version!

The product is compatible from firmware 19.
A downgrade to a version \leq firmware 19 is not permitted.

You can update the firmware in the following ways using:

- WAGOupload
- Memory card and WBM

12.2.1 Use WAGOupload to Update/Downgrade the Firmware



Note

Note the WAGOupload version!

The product is compatible from WAGOupload version 1.14.0.0.

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

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

The newly installed firmware is now available on your controller.

12.2.2 Perform Firmware Update/Downgrade

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

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

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

12.3 Updating Root Certificates

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

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

13 Removal

13.1 Removing Devices



DANGER

Do not work when devices are energized!

High voltage can cause electric shock or burns.

Switch off all power to the device prior to performing any installation, repair or maintenance work.

13.1.1 Remove Controller

Use a tool to lever out the orange DIN-rail release tab until it unlocks with a click.

The DIN-rail release tab then remains in its disengaged position. The DIN-rail release tab does not retract into the housing.

You can now lift the controller vertically upwards from the DIN-rail and remove it.

The DIN-rail release tab automatically jumps back into the housing once the controller is released from the DIN-rail.

14 Disposal

14.1 Electrical and electronic equipment



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

Electrical and electronic equipment contain materials and substances that can be harmful to the environment and health. Electrical and electronic equipment must be disposed of properly after use.

WEEE 2012/19/EU applies throughout Europe. Directives and laws may vary nationally.



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

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

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

14.2 Packaging

Packaging contains materials that can be reused.

PPWD 94/62/EU and 2004/12/EU packaging guidelines apply throughout Europe. Directives and laws may vary nationally.

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

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

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

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

15 Accessories

15.1 Tools

Only use insulated tools.

Table 68: Accessories – Tools

<i>picoMAX</i> ® unlocking tool		2092-1630
Operating tool with partially insulated shaft	Type 1, 2.5 × 0.4 mm blade	210-719

16 Appendix

16.1 Configuration Dialogs

16.1.1 Web-Based-Management (WBM)

16.1.1.1 “Information” Tab

16.1.1.1.1 “Device Status” Page

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

“Device Details” Group

This group shows information about product identification.

Table 69: WBM “Device Status” Page – “Device Details” Group

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

“Network TCP/IP Details” Group

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

Table 70: WBM “Device Status” Page – “Network TCP/IP Details” Group

Parameter	Meaning	
Bridge <n>	Bridge currently configured; the properties are displayed in a separate area for each configured bridge.	
MAC Address	MAC address used for product identification and addressing	
IP Source	Current reference type of the IP address	
	None	No IP allocation method is selected; this occurs, for example, if a bridge was added due to changes to the bridge configuration. Select a source in the Configuration tab on the Networking > TCP/IP Configuration page.
	static IP	Static IP address assignment
	dhcp	Dynamic IP address assignment via DHCP
	bootp	Dynamic IP address assignment via BootP (if BootP is supported)
	external	The IP address may be assigned by the fieldbus application; this occurs e.g., if the IP address is controlled by the application.
IP Address	Current product IP address	
Subnet Mask	Current product subnet mask	

16.1.1.1.2 “Vendor Information” Page

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

16.1.1.1.3 “PLC Runtime Information” Page

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

“Runtime” Group

Table 71: WBM “PLC Runtime Information” Page – “Runtime” Group

Parameter	Explanation
Version	The version of the enabled runtime system is shown. If the runtime system is disabled, “None” is displayed and the subsequent fields of this group are hidden.

“WebVisu” Group

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

16.1.1.1.4 “WAGO Software License Agreement” Page

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

16.1.1.1.5 “Open Source Licenses” Page

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

16.1.1.1.6 “WBM Third Party License Information” Page

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

16.1.1.1.7 “Trademarks Information” Page

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

16.1.1.1.8 “WBM Version” Page

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

16.1.1.2 “Configuration” Tab

16.1.1.2.1 “PLC Runtime Configuration” Page

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

“General PLC Runtime Configuration” Group

Table 72: WBM “PLC Runtime Configuration” Page – “General PLC Runtime Configuration” Group

Parameter	Meaning	
PLC runtime version	Select here the PLC runtime system to be enabled.	
	None	No runtime system is enabled.
	CODESYS V3	CODESYS V3 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

**Only the first partition can be used as the Home directory!**

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

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

The home directory change only takes effect after the product restarts. For this purpose, use the WBM reboot function. Do not switch off the product too early!

“Webserver Configuration” Group

Table 73: WBM “PLC Runtime Configuration” Page – “Webserver Configuration” Group

Parameter	Meaning	
CODESYS V3 Webserver State	This displays the status (enabled/disabled) of the CODESYS V3 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.
	WebVisu	The web visualization of the runtime system is displayed.

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

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

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

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

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

Note



Possible error messages when calling up the web visualization

The “500 – Internal Server Error” message indicates that the Webserver is not enabled.

A page with the header “WebVisu not available” means that no application has been loaded in the product using web visualization.

16.1.1.2.2 “TCP/IP Configuration” Page

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

“TCP/IP Configuration” Group

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

Table 74: WBM “TCP/IP Configuration” Page – “TCP/IP Configuration” Group

Parameter	Meaning	
Network Details Bridge <n>	Settings for the bridge currently configured	
Current IP Address	This displays the current IP address.	
Current Subnet Mask	This displays current subnet mask.	
Current Default Gateway	The IP address of the current default gateway is displayed.	
IP Source	You can specify whether to use a static or dynamic IP address.	
	Static IP	Static IP addressing
	DHCP	Dynamic IP addressing via DHCP
	BootP	Dynamic IP addressing via BootP
	external	The IP address may be assigned by the fieldbus application; this occurs e.g., if the IP address is controlled by the application.
IP Address	Enter a static IP address. This is enabled if “Static IP” is enabled in the IP Source field.	
Subnet Mask	Enter the subnet mask. This is enabled if “Static IP” is enabled in the IP Source field.	
Default Gateway	Enter the IP address of the default gateway here.	

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

“DNS Server” Group

Table 75: WBM “TCP/IP Configuration” Page – “DNS Server” Group

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

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

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

16.1.1.2.3 “Ethernet Configuration” Page

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

“Bridge Configuration” Group

Table 76: WBM “Ethernet Configuration” Page – “Bridge Configuration” Group

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

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

“Switch Configuration” Group

This group only appears if parameter configuration is supported.

Table 77: WBM “Ethernet Configuration” Page – “Switch Configuration” Group

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

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

"Dummy Interfaces" Group

Table 78: WBM "Ethernet Configuration" Page – "Dummy Interfaces" Group

Parameter	Explanation
Name	Name of the selected dummy interface
Add dummy interface	Create a new dummy interface.
Name	Enter the name of the new dummy interface.

To delete a selected entry, click the **[Delete]** button. The changes take effect immediately.

To create a new entry, click the **[Add]** button. The changes take effect immediately.

"VLAN Interfaces" Group

Table 79: WBM "Ethernet Configuration" Page – "VLAN Interfaces" Group

Parameter	Explanation
Name	Name of the selected VLAN interface
VLAN ID	VLAN ID of the selected VLAN interface
Link	Assigned bridge of the selected VLAN interface
Add	Create a new VLAN interface.
Name	Enter the name of the new VLAN interface.
VLAN ID	Enter the VLAN ID; Permissible values are 3 ... 4094.
Link	Select assigned bridge.

To delete a selected entry, click the **[Delete]** button. The changes take effect immediately.

To create a new entry, click the **[Add]** button. The changes take effect immediately.

“Ethernet Interface Configuration” Group

Table 80: WBM “Ethernet Configuration” Page – “Ethernet Interface Configuration” Group

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

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

16.1.1.2.4 Configuration of Host and Domain Name” Page

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

“Hostname” Group

Table 81: WBM “Configuration of Host and Domain Name” Page – “Hostname” Group

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

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

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

The change takes effect immediately.

If the controller has been assigned a host name via DHCP, it is given preference and the manually configured host name is not used.

To accept the manually configured host name, the configuration of the DHCP server may have to be reduced by assigning the host name.

“Domain Name” Group

Table 82: WBM “Configuration of Host and Domain Name” Page – “Domain Name” Group

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

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

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

The change takes effect immediately.

If the controller has been assigned a domain name via DHCP, it is given preference and the manually configured domain name is not used.

To accept the manually configured domain name, the configuration of the DHCP server may have to be reduced by assigning the domain name.

16.1.1.2.5 “Routing” Page

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

“IP Forwarding through multiple interfaces” Group

Table 83: WBM “Routing” Page – “IP Forwarding through multiple interfaces” Group

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

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

“Custom Routes” Group

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

Table 84: WBM “Routing” Page – “Custom Routes” Group

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

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

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

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

“Dynamic Routes” Group

All default gateways received via DHCP are displayed.

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

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

“IP-Masquerading” Group

Each entry has its own area in the display.

Table 85: WBM “Routing” Page – “IP-Masquerading” Group

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

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

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

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

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

“Port-Forwarding” Group

Each entry has its own area in the display.

Table 86: WBM “Routing” Page – “Port Forwarding” Group

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

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

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

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

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

16.1.1.2.1 “Spanning Tree Protocol” Page

The settings for STP/RSTP are shown on the “Spanning Tree Protocol” page.

“Status” Group

The “Status” group displays the current values of the enabled STP/RSTP configuration.

Table 87: WBM “Spanning Tree Protocol” Page – “Status” Group

Parameters	Explanation	
Current Status	Current Status	
	<input type="checkbox"/>	STP/RSTP is disabled.
	<input checked="" type="checkbox"/>	STP/RSTP is enabled.
Current Bridge	Selected Bridge	
Current Mode	Current Protocol	
	STP	Spanning Tree Protocol is enabled.
	RSTP	Rapid Spanning Tree Protocol is enabled.
Current Priority	Current Bridge Priority	
Current Hello Time (sec)	Current “Hello” time in seconds	
Current Forward Delay (sec)	Current “Forward Delay” time in seconds	
Current Max Age (sec)	Current “Max Age Time” in Seconds	
Current Max Hops	Current Max Hops	
Current Path Cost	Current Path Cost	
Port X[n]	A separate area is displayed for each port X[n] of the selected bridge. The port settings are only displayed after STP/RSTP has been successfully enabled.	
Current Bpdu Filter	Current “Bpdu Filter” status	
	<input type="checkbox"/>	Bpdu filter is disabled.
	<input checked="" type="checkbox"/>	Bpdu filter is enabled.
Current Bpdu Guard	Current “Bpdu Guard” status	
	<input type="checkbox"/>	Bpdu Guard is disabled.
	<input checked="" type="checkbox"/>	Bpdu Guard is enabled.
Current Edge Port	Current Port Status	
	<input type="checkbox"/>	Port is not an edge port.
	<input checked="" type="checkbox"/>	Port is an edge port.
Current Root Guard	Hier wird der aktuelle „Root Guard“-Status angezeigt.	
	<input type="checkbox"/>	Root-Guard ist nicht aktiv.
	<input checked="" type="checkbox"/>	Root-Guard ist aktiv.
Current Path Cost	Current path costs	
Current Priority	Current priority	

Table 87: WBM "Spanning Tree Protocol" Page – "Status" Group

Parameters	Explanation	
Current Role	Current role of the port	
	Designated	The port selected in each LAN segment that offers the lowest root path cost. The higher the connection speed, the lower the cost value.
	Disabled	The port is disabled.
Current Status	Current port status	
	Forwarding	The port can send and receive data, learn MAC addresses and forward data to its destination.
	Discarding	The port does not forward data to other switches in the network and does not update MAC address tables.

"Parameter Settings" Group

In the "Parameter Settings" group, you can change the settings for the STP/RSTP configuration.

Table 88: WBM "Spanning Tree Protocol" Page – "Parameter Settings" Group

Parameters	Explanation	
Enabled	Enable/disable Spanning Tree Protocol.	
	<input type="checkbox"/>	Spanning Tree Protocol is disabled.
	<input checked="" type="checkbox"/>	Spanning Tree Protocol is enabled.
Bridge	Select bridge.	
Mode	Select protocol.	
	STP	Spanning Tree Protocol
	RSTP	Rapid Spanning Tree Protocol
Priority	Set bridge priority; Permissible values: 1 ... 15	
Hello Time	Set Hello Time; Permissible Values: 1 ... 19	
Forward Delay	Set forward delay; Permissible values: 4 ... 30	
Max Age	Set max age; Permissible values: 6 ... 40	
Max Hops	Set max hops; Permissible values: 6 ... 40	
Port X[n]	Each port X[n] has its own area. The port settings are only available after STP/RSTP has been successfully enabled.	

Table 88: WBM "Spanning Tree Protocol" Page – "Parameter Settings" Group

Parameters	Explanation	
Bpdu Filter	Enable/disable Bpdu filter.	
	<input type="checkbox"/>	Bpdu filter is disabled.
	<input checked="" type="checkbox"/>	Bpdu filter is enabled.
Bpdu Guard	Enable/disable the Bpdu Guard.	
	<input type="checkbox"/>	Bpdu Guard is disabled.
	<input checked="" type="checkbox"/>	Bpdu Guard is enabled.
Edge Port	Enable/disable port as edge port.	
	<input type="checkbox"/>	Port is not an edge port.
	<input checked="" type="checkbox"/>	Port is an edge port.
Root Guard	Enable/disable root guard.	
	<input type="checkbox"/>	Root Guard is disabled.
	<input checked="" type="checkbox"/>	Root Guard is enabled.
Path Cost	Set Path Cost; Permissible Values: 0 ... 65535	
Priority	Set priority; Permissible values: 0 ... 15, Default = 8	

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

16.1.1.2.2 “Clock Settings” Page

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

“Timezone and Format” Group

Table 89: WBM “Clock Settings” Page – “Timezone and Format” Group

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

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

“UTC Time and Date” Group

Table 90: WBM “Clock Settings” Page – “UTC Time and Date” Group

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

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

“Local Time and Date” Group

Table 91: WBM “Clock Settings” Page – “Local Time and Date” Group

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

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

16.1.1.2.3 “Create Bootable Image” Page

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

“Create bootable image from boot device” Group

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

Table 92: WBM “Create Bootable Image” Page – “Create bootable image from active partition” Group

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

- Free space on target device:
If the available memory space is less than 5% a warning is displayed. You can still start the copy process despite the warning. If the available space is too low, a corresponding message is displayed and copying cannot be started.
- Device being used by CODESYS:
If the device is being used by CODESYS, a warning is displayed. Although it is not recommended, you can still start the copying procedure despite this warning.

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

16.1.1.2.4 “Firmware Backup” Page

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

“Firmware Backup” Group

Table 93: WBM “Firmware Backup” Page – “Firmware Backup” Group

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

Note



Note the firmware version!

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

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

Note**Only one package may be copied to the network!**

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

Note**No backup of the memory card!**

Backup from the memory card to the internal flash memory is not possible.

Note**Account for backup time!**

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

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

16.1.1.2.5 “Firmware Restore” Page

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

“Firmware Restore” Group

Table 94: WBM “Firmware Restore” Page – “Firmware Restore” Group

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

Note



Note the firmware version!

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

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

Note**File size must not exceed the size of the internal drive!**

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

Note**Restoration only possible from internal memory!**

If the device was booted from the memory card, the firmware cannot be restored.

Note**Reset by restore**

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

Note**Connection loss through restore**

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

Note**Note the restore time!**

The restore process takes approx. 2 ... 3 minutes.

After the restore process, the controller is restarted and is then ready for use again.

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

16.1.1.2.6 “Active System” Page

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

“Boot Device” Group

Table 95: WBM “Active System” Page – “Boot Device” Group

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

“System <n> (Internal Flash)” Groups

Table 96: WBM “Active System” Page – “System <n> (Internal Flash)” Group

Table 66: WDM Active System Page - System ID (Internal Patch) Group		
Parameter	Explanation	
Active	This shows whether the system is active.	
Configured	This shows whether the system should be active after the next reboot.	
State	The system status is displayed here.	
	good	The system is valid and can be used.
	bad	The system is not valid and cannot be used.

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



Note

Provide a bootable system!

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

16.1.1.2.7 “Mass Storage” Page

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

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

“Devices” Group

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

Table 97: WBM “Mass Storage” Page – “Devices” Group

Parameter	Explanation
<Device>	The storage medium is displayed.
Boot device	This shows whether the device has booted from this storage medium.
Volume name	The name of the storage medium is displayed.

“Create new Filesystem on Memory Card” Group

Table 98: WBM “Mass Storage” Page – “Create new Filesystem on Memory Card” Group

Parameter	Meaning	
Filesystem type	You can select the format in which the filesystem should be created on the memory card.	
	Ext4	The filesystem is created in Ext4 format. The files are not readable under Windows!
	FAT	The filesystem is created in FAT format.
Label	Specify the name for the storage medium when formatted.	

**Note****Data is deleted!**

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

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

16.1.1.2.8 “Software Uploads” Page

On “Software Upload” page, you can install software packages (IPK files) on the product from your PC.



Note

Install IPK files from trusted sources only!

IPK files are installed with extended rights (root rights), as long as not stated otherwise in the metadata.

Be careful when installing IPK files and install them from trusted sources only.

Table 99: WBM “Software Uploads” Page – “Upload New Software” Group

Parameters	Explanation
Software file	The file name of your selected software package is displayed, as long as you have not yet transferred it to the product. If you have not yet selected a package, “Choose ipk file...” appears. Click the input field and select a file with a software package on your PC.

To install the package, click **[Install]**.

The file with the software package is deleted from the device again after the installation process. If this is not possible due to a processing error, it is deleted no later than the next time the product restarts.

16.1.1.2.9 “Configuration of Network Services” Page

The settings for various services are shown on the “Configuration of Network Services” page.



Note

Close any ports and services that you do not need!

Unauthorized persons may gain access to your automation system through open ports.

To reduce the risk of cyber attacks and thus increase cyber security, close all ports and services not required by your application in the control components (e.g., port 6626 for WAGO-I/O-CHECK and port 11740 for CODESYS V3). Only open ports and services during commissioning and/or configuration.

“FTP” Group

Table 100: WBM “Configuration of Network Services” Page – “FTP” Group

Parameter	Explanation
Service active	Enable/disable the FTP service. This service is disabled by default.

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

“FTPES (explicit FTPS)” Group

Table 101: WBM “Configuration of Network Services” Page – “FTPES (explicit FTPS)” Group

Parameter	Explanation
Service active	Enable/disable the FTPS service. This service is disabled by default.

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

“HTTP” Group

Table 102: WBM “Configuration of Network Services” Page – “HTTP” Group

Parameter	Explanation
Service active	Enable/disable the HTTP service. This service is disabled by default.

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



Note

Disconnection abort on disabling

If the HTTP service is disabled, the connection to the product may be interrupted. In that case, reopen the page.

“HTTPS” Group

Table 103: WBM “Configuration of Network Services” Page – “HTTPS” Group

Parameter	Explanation
Service active	State of HTTPS service is displayed here.

“I/O-CHECK” Group

This group appears if the controller supports WAGO-I/O-CHECK.

Table 104: WBM “Configuration of Network Services” Page – “I/O-CHECK” Group

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

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

16.1.1.2.10 “Configuration of NTP Client” Page

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

“NTP Client Configuration” Group

Table 105: WBM “Configuration of NTP Client” Page – “NTP Client Configuration” Group

Parameters	Explanation
Service enabled	Enable/disabled time update.
Update interval (sec)	Specify the update interval of the time server.
Time Server <n>	Enter here the IP addresses of up to 4 time servers. Time server No. 1 is queried first. If no data is accessible via this server, time server No. 2 is queried, etc.
Additionally assigned (DHCP)	The NTP servers assigned if necessary by DHCP (or BootP) are displayed. If no NTP server has been assigned by DHCP (or BootP), “(No additional servers assigned)” is displayed.

To update the time regardless of interval, click the **[Update Time]** button.

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

16.1.1.2.11 “PLC Runtime Services” Page

The settings for various services of the runtime systems are displayed on the “PLC Runtime Services” page.

“CODESYS V3” Group

This group only appears if the controller supports the CODESYS V3 runtime system.

Table 106: WBM “PLC Runtime Services” Page – “CODESYS V3” Group

Parameter	Explanation
CODESYS V3 State	This displays the status (enabled/disabled) of the CODESYS V3 runtime system.
Webserver enabled	Enable or disable the Webserver for the CODESYS V3 web visualization.
Seperated WebVisu ports (8080/8081)	Enter here whether the CODESYS V3 web visualization is provided on ports 8080/8081. By default the web visualization is provided on WBM ports 80/443.
Port authentication enabled	Enter here whether a login is required for connecting to the device. The user name is admin and the password specified at “General Configuration.”

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

The change in authentication takes effect after the next restart.

All other changes take effect immediately.

16.1.1.2.12 “SSH Server Settings” Page

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

“SSH Server” Group

Table 107: WBM “SSH Server Settings” Page – “SSH Server” Group

Parameters	Explanation
Service active	You can enable/disable the SSH server.
Port Number	Enter the port number.
Allow root login	You can enable or inhibit root access.
Allow password login	Enable or disable the password query function.

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

16.1.1.2.1 “DHCP Server Configuration” Page

The “DHCP Server Configuration” page displays the DHCP service settings.

“DHCP Server Configuration Bridge <n>” Group

Table 108: WBM “DHCP Server Configuration” Page – “DHCP Configuration Bridge <n>” Group

Parameter	Explanation
Service active	Enable or disable the DHCP service for the interface X<n>.
Start IP for Range	Enter the start value of the available IP address range.
End IP for Range	Enter the end value of the available IP address range.
Lease time (min)	Specify the lease time here in seconds. 120 minutes are entered by default.
Static Hosts	This displays the static assignments of MAC IDs to IP addresses. If no assignment was defined, “No static hosts configured” is displayed.
Add Static Host	You can add static MAC addresses or host names and IP addresses.
MAC Address or Hostname	Enter a new static assignment, e.g., “01:02:03:04:05:06=192.168.1.20” or “hostname=192.168.1.20”. You can enter 15 assignments or host names.
Ip Address	Enter the IP address. You can enter 15 IP addresses.

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

To accept a new assignment click the **[Add]** button. The change takes effect immediately.

Click **[Delete]** to delete an existing assignment. The change takes effect immediately.

16.1.1.2.2 “Configuration of DNS Server” Page

The “Configuration of DNS Server” page displays the DNS service settings.

“DNS Server” Group

Table 109: WBM “Configuration of DNS Server” Page – “DNS Server” Group

Parameter	Explanation	
Service active	You can enable/disable the DNS server service.	
Mode	Select the operating mode of the DNS server.	
	Proxy	Requests are buffered to optimize throughput.
	Relay	All requests are routed directly.
Static Hosts	This displays the names for IP addresses. If no assignment was defined, “No static hosts configured” is displayed.	
Add Static Host	You can add static IP addresses and host names below.	
IP Address	Enter a new static assignment, e.g., “192.168.1.20:hostname”. You can enter 10 assignments.	
Hostname	Enter a host name.	

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

To accept a new assignment click the **[Add]** button. The change takes effect immediately.

Click **[Delete]** to delete an existing assignment. The change takes effect immediately.

16.1.1.2.3 “Status overview” Page

On the “Status overview” page, you can find information about cloud access.

“Connection <n>” Group

A group is displayed for each cloud access.

Table 110: WBM “Status Overview” Page – “Connection <n>” Group

Parameter	Explanation
Is Active	The status of the cloud connectivity application is displayed.
Data from PLC Runtime	This shows how many data collections have been registered on the IEC application side for transfer to the cloud.
Cloud Connection	The status of the connection to the cloud service is shown.
Heartbeat	This shows the current heartbeat interval setting in seconds.
Telemetry Data Transmission	This indicates whether transfer of data is enabled or disabled.
Cache fill level (QoS 1 and 2)	This shows the fill level of the memory cache for outgoing messages as a percentage.

“Diagnosis” Group

This group is visible only when diagnostic information is available.

Warnings and errors are displayed here, along with information (when available) on how to potentially eliminate the error(s).

16.1.1.2.4 “Configuration of Connection <n>” Page

You can find settings and information for cloud access on the “Configuration of Connection <n>” page.

A page is displayed for each cloud access.

“Configuration” Group

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

The dependencies are shown in a separate table.

Table 111: WBM “Configuration of Connection <n>” Page – “Configuration” Group

Parameter	Explanation
Enabled	You can enable/disable the cloud connectivity function.
Cloud platform	Select the cloud platform.
Hostname	Enter the host name or IP address for the selected cloud platform.
ID Scope	Enter the end point for the Azure Device Provisioning Service (DPS).
Registration ID	Enter the Registration ID for the Azure Device Provisioning Service (DPS).
Port number	Enter the port here to which a connection is to be established. Typical values are 8883 for encrypted connections and 1883 for unencrypted connections.
Device ID	Enter the device ID for the selected cloud platform.
Client ID	Enter the client ID for the selected cloud platform.
Authentication	Select the authentication method. Possible settings are “Shared Key Access” or “X.509 Certificate”.
Activation Key	Enter the activation key for the selected cloud platform.
Clean Session	Specify whether clean session should be enabled during the connection to the cloud service. If clean session is enabled, the information and messages on this connection are not stored persistently on the cloud service.
TLS	You can specify whether TLS encryption should be used for the connection to the cloud platform. Amazon Web Services (AWS) always uses TLS.

Table 111: WBM "Configuration of Connection <n>" Page – "Configuration" Group

Parameter	Explanation
CA file	Enter the path here to the file encoded in PEM format that contains the trusted CA certificate to use to establish an encrypted connection. The default value is the CA certificate /etc/ssl/certs/ca-certificates.crt that is already installed on the controller.
Users	Enter the user name for cloud service authentication.
Password	Enter the password for cloud service authentication.
Certification file	Enter the path here to the file encoded in PEM format that is used for cloud service authentication.
Key file	Enter the path to the file encoded in PEM format that contains the private key for cloud service authentication.
Use websockets	Here, you can specify whether the connection to the cloud platform is to be set up using the WebSocket protocol via Port 443. If this checkbox is not selected, the connection to the cloud platform is set up using the MQTT protocol via Port 8883.
Proxy Type	Select which type of proxy should be used.
HTTP Proxy Host	Enter the host name or IP address of the proxy.
HTTP Proxy Port	Enter the port number of the proxy.
HTTP Proxy User	Enter the name of the proxy user.
HTTP Proxy Password	Enter the password for the proxy user.
Use compression	Here, you can set whether the data is to be compressed using GZIP compression.
Data Protocol	Here you can select the data protocol.
Cache mode	Specify in which memory the cache for the data telegrams should be created. This selection field is only enabled if a correctly formatted SD card is inserted (more information is available in Application Note A500920).
Last Will	You can specify whether a last will message should be enabled/disabled.
(Last Will) Topic	You can specify the topic under which the last will messages should be sent.
(Last Will) Message	You can enter the message you wish to use as the last will message.
(Last Will) QoS	You can specify the "Quality of Service" (QoS) of the last will message.
(Last Will) Retain	Here, you can set whether the previous last-will message sent under a topic from the broker is to be handled as a retained message.

Table 111: WBM "Configuration of Connection <n>" Page – "Configuration" Group

Parameter	Explanation
Device info	Specify whether a device info message should be generated that informs the cloud service of the basic configuration of the controller (more information is available in the Application Note A500920).
Device status	Specify whether device state messages should be generated that inform the cloud service about changes in the mode selector switch and the LEDs (more information is available in the Application Note A500920).
Standard commands	Specify whether the integrated standard commands should be supported (list of standard commands is available in the Application Note A500920). If the checkbox is disabled, only the commands defined in the IEC program are supported.
Application property template	<p>You have the option of creating your own property for the individual MQTT messages to the Azure cloud.</p> <p>This parameter is optional; i.e., if the field is left blank, this property is not sent.</p> <p>The following placeholders are available to create this property:</p> <ul style="list-style-type: none"> • <m>: Message type • <p>: Protocol version • <d>: Device ID <p>Examples:</p> <ul style="list-style-type: none"> • MyKey=HelloWorld_<m> • TestKey=<m>/<p>/<d> • DeviceId=<d>

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

The changes only take effect after the controller restarts. For this purpose, use the WBM reboot function. Do not shut down the controller too early!

The following tables show the dependencies of the selection and input fields as well as the possible settings.

Table 112: Display of the Selection and Input Fields Depending on the Selected Cloud Platform

Selection or Input Field	Cloud Platform					
	WAGO Cloud	Azure	MQTT AnyCloud	Amazon Web Services	SAP IoT Services	Azure Device Provisioning Service (DPS)
Enabled	X	X	X	X	X	X
Cloud platform	X	X	X	X	X	X
Hostname	X	X	X	X	X	

Table 112: Display of the Selection and Input Fields Depending on the Selected Cloud Platform

Selection or Input Field	Cloud Platform					
	WAGO Cloud	Azure	MQTT AnyCloud	Amazon Web Services	SAP IoT Services	Azure Device Provisioning Service (DPS)
Port number			X	(X)	X	
Device ID	X	X				
Client ID			X	X	X	
Authentication		X				X
Activation Key	X	X2				X2
Clean Session			X	(X)	X	
TLS			X	(X)	X	
CA file			X	X	X	X
User			X			
Password			X			
Certification file		X2	X	X	X	
Key file		X2	X	X	X	
Use websockets	X	X1				X
Proxy Type	X4	X4				X4
HTTP Proxy Host	X5	X5				X5
HTTP Proxy Port	X5	X5				X5
HTTP Proxy User	X5	X5				X5
HTTP Proxy Password	X5	X5				X5
Data Protocol		X	X	X	(X)	X
Use compression	X	X1	X1			X1
Cache mode	X	X	X	X	X	X
Last Will			X	X	X	
Last Will Topic			X3	X3	X3	
Last Will Message			X3	X3	X3	
Last Will QoS			X3	X3	X3	
Last Will Retain			X3	(X3)	X3	
Device info		X1	X1	X1		X1
Device status		X1	X1	X1		X1
Standard commands		X1	X1	X1		X1
Application property template		X1				X1

Table 112: Display of the Selection and Input Fields Depending on the Selected Cloud Platform

Selection or Input Field	Cloud Platform					
	WAGO Cloud	Azure	MQTT AnyCloud	Amazon Web Services	SAP IoT Services	Azure Device Provisioning Service (DPS)

X: Visible and enabled

(X): Visible, but disabled

X1: Visible and enabled, depending on the selected data protocol

X2: Visible and enabled, depending on the selected authentication

X3: Visible and enabled when “Last Will” is switched on

(X3): Visible, but disabled when “Last Will” is switched on

X4: Enabled if “Use websockets” is switched on.

X5: Visible and enabled if “Use websockets” is switched on and if “HTTP” is set as the “Proxy Type”.

Table 113: Choice of Data Protocol Depending on the Selected Cloud Platform

Data Protocol	Cloud Platform					
	WAGO Cloud	Azure	MQTT AnyCloud	Amazon Web Services	SAP IoT Services	Azure Device Provisioning Service (DPS)
WAGO Protocol		X	X	X		X
WAGO Protocol 1.5		X	X	X		X
Native MQTT			X	X	(X)	
Sparkplug payload B		X	X	X		

X: Selection possible

(X): Fixed setting

Table 114: Display of the Selection and Input Fields Depending on the Selected Data Protocol

Selection or Input Field	Data Protocol			
	WAGO Protocol	WAGO Protocol 1.5	Native MQTT	Sparkplug payload B
Client ID	X	X	X	X
Use compression	X	X	X	
Device info	X	X		
Device status	X	X		
Standard commands	X	X		
Application property template	X	X		

X: Visible and enabled

Table 115: Choice of Cache Mode Depending on the Selected Data Protocol

Cache Mode	Data Protocol			
	WAGO Protocol	WAGO Protocol 1.5	Native MQTT	Sparkplug payload B
RAM	X	X	X	(X)
SD-Card	X1	X1	X1	

X: Selection possible

X1: Selection only possible if "Compression" is not switched on

(X): Fixed setting

Table 116: Display of the Selection and Input Fields Depending on the Selected Authentication

Selection or Input Field	Authentication	
	Shared Access Key	X.509 Certificate
Activation Key	X	
Certification file		X
Key file		X

X: Visible and enabled

16.1.1.2.5 “Configuration of General SNMP Parameters” Page

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

“General SNMP Configuration” Group

Table 117: 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).
ObjectID	Enter here the object ID (sysOID).

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

16.1.1.2.6 “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.

“Communities” Group

Table 118: WBM “Configuration of SNMP v1/v2c Parameters” Page – “Communities” Group

Parameters	Explanation
Community <n>	Each configured community has its own area in the display. If no community has been configured, “(no Communities configured)” is displayed.
Name	The community name for the SNMP manager configuration is displayed. 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.
Access	This displays the access rights for the community. Possible values: “ReadOnly” or “ReadWrite”.
Add new Community	In this area, you can enter a new community.
Name	Specify the community name for the SNMP manager configuration. (See above) 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.”
Access	Specify the access rights for the new community. Possible values: “ReadOnly” or “ReadWrite”.

Click the corresponding **[Delete]** button to delete an existing community.

Click the **[Add]** button to add a new community.

“Trap Receivers” Group

Table 119: WBM “Configuration of SNMP v1/v2c Parameters” Page – “Trap Receivers” Group

Parameters	Meaning
Trap Receiver <n>	Each configured trap receiver has its own area in the display. If no trap receiver has been configured, “(no Trap Receivers configured)” is displayed.
Host	The host name or the IP address for the trap receiver (management station) is displayed.
Community Name	This displays the community name for the trap receiver configuration. The community name can be evaluated by the trap receiver.
Version	This displays the SNMP version, via which the traps are sent.
Add new Trap Receiver	In this area, you can enter a new trap receiver.
Host	Specify the host name or the IP address for the new trap receiver (management station).
Community Name	Specify the community name for the new trap receiver configuration. (See above). 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. Possible values: “v1” or “v2c”.

Click the corresponding **[Delete]** button to delete an existing trap receiver.

Click the **[Add]** button to add a new trap receiver.

16.1.1.2.7 “Configuration of SNMP v3 Parameters” Page

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

“Users” Group

Table 120: WBM “Configuration of SNMP v3 Parameters” Page – “Users” Group

Parameters	Meaning
User <n>	Each configured v3 user has its own area in the display. If no v3 user has been configured, “(no Users configured)” is displayed.
Security Authentication Name	The user name is displayed.
Authentication Type	The authentication type for the SNMP v3 packets is displayed. Possible values: - Use no authentication (“None”) - Message Digest 5 (“MD5”) - Secure Hash Algorithm (“SHA”, “SHA224”, “SHA256”, “SHA384”, “SHA512”)
Authentication Key	The authentication key is displayed.
Privacy	The encryption algorithm for the SNMP message is displayed. Possible values: - No encryption (“None”) - Data Encryption Standard (“DES”) - Advanced Encryption Standard (“AES”, “AES128”, “AES192”, “AES192C”, “AES256”, “AES256C”)
Privacy Key	The key for encryption of the SNMP message is displayed. If nothing is displayed, the “authentication key” is automatically used.
Access	This displays the access rights for the user. Possible values: “ReadOnly” or “ReadWrite”.
Add new v3 User	In this area, you can enter a new v3 user. You can create up to 10 users.
Security Authentication Name	Enter the user name. This name must be unique; a pre-existing user name is not accepted when entered. The name must be min. 8 and max. 32 characters long and contain lower case letters (a ... z), upper case letters (A ... Z), numbers (0 ... 9), special characters !()*~'._- but no spaces.
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”, “SHA224”, “SHA256”, “SHA384”, “SHA512”)

Table 120: WBM "Configuration of SNMP v3 Parameters" Page – "Users" Group

Parameters	Meaning
Authentication Key	Specify the authentication key. The key must be min. 8 and max. 32 characters long and contain lower case letters (a ... z), upper case letters (A ... Z), numbers (0 ... 9), special characters !()*~'.- _ but no spaces.
Privacy	Specify the encryption algorithm for the SNMP message. Possible values: - No encryption ("None") - Data Encryption Standard ("DES") - Advanced Encryption Standard ("AES", "AES128", "AES192", "AES192C", "AES256", "AES256C")
Privacy Key	Enter the key for encryption of the SNMP message. If nothing is specified here, the "authentication key" is automatically used. The key must be min. 8 and max. 32 characters long and contain lower case letters (a ... z), upper case letters (A ... Z), numbers (0 ... 9), special characters !()*~'.- _ but no spaces.
Access	Specify the access rights for the new user. Possible values: "ReadOnly" or "ReadWrite".

Click the respective **[Delete]** button to delete an existing user.

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

“Trap Receivers” Group

Table 121: WBM “Configuration of SNMP v3 Parameters” Page – “Trap Receivers” Group

Parameters	Meaning
Trap Receiver <n>	Each configured v3 trap receiver has its own area in the display. If no v3 trap receiver has been configured, “(no Trap Receivers configured)” is displayed.
Security Authentication Name	The user name is displayed.
Authentication Type	The authentication type for the SNMP v3 packets is displayed. Possible values: - Use no authentication (“None”) - Message Digest 5 (“MD5”) - Secure Hash Algorithm (“SHA”, “SHA224”, “SHA256”, “SHA384”, “SHA512”)
Authentication Key	The authentication key is displayed.
Privacy	The encryption algorithm for the SNMP message is displayed. Possible values: - No encryption (“None”) - Data Encryption Standard (“DES”) - Advanced Encryption Standard (“AES”, “AES128”, “AES192”, “AES192C”, “AES256”, “AES256C”)
Privacy Key	The key for encryption of the SNMP message is displayed. If nothing is displayed, the “authentication key” is automatically used.
Host	The host name or the IP address of a trap receiver for v3 traps is displayed.
Add new Trap Receiver	In this area, you can enter a new v3 trap receiver. You can create up to 10 trap receivers.
Security Authentication Name	Enter the user name. This name must be unique; a pre-existing user name is not accepted when entered. The name must be min. 8 and max. 32 characters long and contain lower case letters (a ... z), upper case letters (A ... Z), numbers (0 ... 9), special characters !()*~'._- but no spaces.
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”, “SHA224”, “SHA256”, “SHA384”, “SHA512”)

Table 121: WBM "Configuration of SNMP v3 Parameters" Page – "Trap Receivers" Group

Parameters	Meaning
Authentication Key	Specify the authentication key. The key must be min. 8 and max. 32 characters long and contain lower case letters (a ... z), upper case letters (A ... Z), numbers (0 ... 9), special characters !()*~'.- _ but no spaces.
Privacy	Specify the encryption algorithm for the SNMP message. Possible values: - No encryption ("None") - Data Encryption Standard ("DES") - Advanced Encryption Standard ("AES", "AES128", "AES192", "AES192C", "AES256", "AES256C")
Privacy Key	Enter the key for encryption of the SNMP message. If nothing is specified here, the "authentication key" is automatically used. The key must be min. 8 and max. 32 characters long and contain lower case letters (a ... z), upper case letters (A ... Z), numbers (0 ... 9), special characters !()*~'.- _ but no spaces.
Host	Specify the host name or the IP address for a trap receiver for v3 traps.

Click the respective **[Delete]** button to delete an existing trap receiver.

Click **[Add]** to add a new trap receiver.

16.1.1.2.1 “Commissioning Settings” Page

The “Commissioning Settings” page contains information and settings for the “Commissioning Agent” service.

“Commissioning” Group

Table 122: WBM “Commissioning Settings” Page – “Commissioning” Group

Parameters	Explanation	
Service Enabled	Enable/disable “Commissioning Agent” service	
	<input type="checkbox"/>	The “Commissioning Agent” service is disabled.
	<input checked="" type="checkbox"/>	The “Commissioning Agent” service is enabled.
Commissioning State	Current status of the “Commissioning Agent” service	
	inactive	The service is disabled.
	searching	The service is looking for a server.
	requesting	The service has found a server and is attempting to connect.
	awaiting response	The service is waiting to be accepted by the server.
	no server found	The service did not find a valid server within the given time of five minutes. To restart the scan, the device must be restarted.
	processing	The service starts installing packages received from the server.
	error exit	The service aborted the installation due to an internal error.
	success	The service has successfully completed the installation.
Connected Server	Domain of the server to which the product is connected; If the product is not connected, “-” is displayed.	

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

16.1.1.2.2 Page “**Docker Settings**”

On the page “Docker Settings”, see the settings for the “Docker®” service.

Group “**Docker Status**”

Table 123: WBM Page “Docker Settings” – group “Docker Status”

Parameter	Meaning	
Current State	The current status of the “Docker®” service is displayed.	
	stopped	The “Docker®” service is disabled.
	running	The “Docker®” service is enabled.
Service Enabled	If you want to enable the “Docker®” service, check this box.	

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

16.1.1.2.3 “WBM User Configuration” Page

The settings for user administration are displayed on the “WBM User Configuration” page.

“Change Password” Group



Note

Changing Passwords

The initial passwords as delivered are documented in this manual and therefore do not provide sufficient protection. Change the passwords to meet your particular needs!

Table 124: WBM “WBM User Configuration” Page – “Change Password” Group

Parameter	Explanation
Old Password	Enter the current password here for authentication.
New Password	Enter the new password here. Permitted characters for the password are the following ASCII characters: a ... z, A ... Z, 0 ... 9, and special characters: ! " # \$ % & ' () * + , . / : ; < = > ? @ [] ^ _ ` { } ~ - .
Confirm Password	Enter the new password again here for confirmation.

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



Note

Note the permitted characters for WBM passwords!

If passwords with invalid characters are set for the WBM outside the WBM (e.g., from a USB keyboard), access to the pages directly on the display is no longer possible because only permitted characters are available from the virtual keyboard.



Note

General Rights of WBM Users

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

User administration for controller applications is configured and managed separately.

16.1.1.3 “Fieldbus” Tab

16.1.1.3.1 “OPC UA Configuration” Page

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

“OPC UA Server Configuration” Group

Table 125: WBM “OPC UA Configuration” Page – “OPC UA Server Configuration” Group

Parameter	Explanation
Enabled	Enable or disable the WAGO OPC UA Server here.
Log level	Select the log level. The following values can be set: Info / Debug / Warning / Error. With log level “Error,” only error messages are read out; with log level “Info,” status messages are read out too. The specific log level selection affects server reaction time. Therefore, select the lowest level necessary; e.g., “Debug” for in-depth analyses.
Ctrl Configuration name	Enter the configuration names the controller contains in the PLC Open Device Set.

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

“OPC UA Server Security Settings” Group

Table 126: WBM “OPC UA Configuration” Page – “OPC UA Server Security Settings” Group

Parameter	Explanation
Anonymous Access	Permit anonymous access to the server. This requires that runtime port authentication also be deactivated.
Allow Password On Plaintext	Transfer of password in readable format
Security Modes	<p>Security Mode of the OPC UA Server Depending on the operating mode you select, different OPC UA endpoints for setting up the connection are available:</p> <p>None: Only the OPC UA endpoint None is activated. This allows an unsecured connection to the OPC UA server to be established.</p> <p>None + Sign + SignAndEncrypt: The endpoints None, Sign and SignAndEncrypt are available. Sign provides an endpoint that is password protected. SignAndEncrypt specifies an endpoint that provides both a password and encryption.</p> <p>Sign + SignAndEncrypt: The Sign and SignAndEncrypt endpoints are available.</p> <p>SignAndEncrypt: Only the SignAndEncrypt endpoint is available.</p>
Security Policies	<p>Selection of security policies Here, you can set the encryption level for the OPC UA server. The following options are available for this:</p> <p>Aes128Sha256RsaOaep and better, Basic256Sha256 and better, Aes256Sha256RsaPss.</p>

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

16.1.1.3.1 “BACnet Status” Page

The “BACnet Status” page displays specific information about your product for the BACnet fieldbus and the BACnet license.

“BACnet Information” Group

Table 127: WBM “BACnet Status” Page – “BACnet Information” Group

Parameters	Explanation	
State	BACnet Fieldbus Status	
	<input type="checkbox"/>	Fieldbus BACnet is disabled.
	<input checked="" type="checkbox"/>	Fieldbus BACnet is enabled.
Mode	BACnet operating mode	
	lp	Communication via BACnet/IP
	sc	Communication via BACnet/SC
Version	Installed BACnet version	
Status Info	BACnet Fieldbus Status	
Device-ID	Current product device ID	

“BACnet License” Group

Table 128: WBM “BACnet Status” Page – “BACnet License” Group

Parameters	Explanation
Type	Display of BACnet licenses
User Objects	Display of the number of existing and possible BACnet objects with the license

“BACnet Data Link” Group

Table 129: WBM “BACnet Status” Page – “BACnet Data Link” Group

Parameters	Explanation
Connection Info	Display of the connection status

16.1.1.3.2 “BACnet Configuration” Page

You can make special settings for the BACnet fieldbus on this page.

“Restart” Group

Table 130: WBM “BACnet Data Link” Page – “BACnet Restart” Group

Parameters	Explanation
[Restart]	Restart the BACnet service

“BACnet Service” Group

Table 131: WBM “BACnet Configuration” Page – “BACnet Service” Group

Parameters	Explanation
Service active	Enable/disable fieldbus BACnet.
	<input type="checkbox"/> BACnet is disabled.
	<input checked="" type="checkbox"/> BACnet is enabled.
Mode	Select the BACnet operating mode here.
	lp Communication via BACnet/IP
	sc Communication via BACnet/SC
Who-Is online interval time (sec)	Time interval between controller requests to the fieldbus and which other subscribers are online (minimum: 60 sec).
Broadcast I-Am answer	Enable/disable the device's I-Am messages to be sent to the BACnet broadcast address.
	<input type="checkbox"/> I-Am messages are not sent to the BACnet broadcast address.
	<input checked="" type="checkbox"/> I-Am messages are sent to the BACnet broadcast address.

Click the **[Submit]** button to apply a change. The change is only applied after the controller is restarted or after a BACnet restart.

“BACnet Data” Group

Table 132: WBM “BACnet Configuration” Page – “BACnet Data” Group

Parameters	Explanation
Delete Persistence Data	Persistent BACnet data is deleted on the next restart.
Reset all BACnet Data and Settings to Default	BACnet-specific settings and data are reset to factory settings the next time you restart.
override.xml Chose file ...	Select the required file on the PC.
[Upload]	Transfer the selected file from the PC to the controller.

Click the **[Submit]** button to apply a change. The change is only applied after the controller is restarted or after a BACnet restart.

“BACnet Log Level” Group

Table 133: WBM “BACnet Configuration” Page – “BACnet Log Level” Group

Parameters	Explanation
Error	Enable/disable error log outputs.
Warning	Enable/disable warning log outputs.
Info	Enable/disable info log output.
Debug	Enable/disable debug log output.

Click the **[Submit]** button to apply a change. The change is only applied after the controller is restarted or after a BACnet restart.

“BACnet Network Capture” Group

Table 134: WBM “BACnet Configuration” Page – “BACnet Network Capture” Group

Parameters	Explanation
Enable	Enable/disable logging of network traffic with the corresponding BACnet filters.
Log pre-master secrets	Enable/disable saving of secrets for decryption of BACnet/SC network traffic.
BACnet Network Capture Archive [Download]	Click the [Download] button to download the logged network traffic, including the secrets, from the device if the option is enabled.

Click the **[Submit]** button to apply a change. The change is only applied after the controller is restarted or after a BACnet restart.

16.1.1.3.3 “BACnet Data Link” Page**“BACnet Restart” Group**

Table 135: WBM “BACnet Data Link” Page – “BACnet Restart” Group

Parameters	Explanation
[Restart]	Restart the BACnet service.

“BACnet/IP” Group

Table 136: WBM “BACnet Data Link” Page – “BACnet/IP” Group

Parameters	Explanation
Port number	Input of the port for BACnet/IP communication

Click the **[Submit]** button to apply a change. The change is only applied after the controller is restarted or after a BACnet restart.

“BACnet/SC” Group

Table 137: WBM “BACnet Data Link” Page – “BACnet/SC” Group

Parameters	Explanation
Mode	Selection of the BACnet/SC operating mode
	Node The device is operated as a BACnet/SC node.
	Primary Hub The device is operated as a BACnet/SC Primary HUB.
	Failover Hub The device is operated as a BACnet/SC Failover HUB.
Port number	Input of the port for BACnet/SC communication
Primary Hub URI	Input of the URI for the primary HUB; wss://<IP address>:<port of the HUB> or wss://<domain name>:<port of the HUB> (e.g., wss://192.168.178.19:47808 or wss://PFC200V3-XXXXXX.localdomain.lan:47808)
Failover Hub URI	Enter the URI for the failover HUB; wss://<IP address>:<port of the HUB> or wss://<domain name>:<port of the HUB> (e.g., wss://192.168.178.19:47808 or wss://PFC200V3-XXXXXX.localdomain.lan:47808)
Allow self signed certificates	Enable/disable whether communication can be established via self-signed certificates.
Allow expired certificates	Enable/disable whether communication via expired certificates can be established.
Accept any certificates	Enable/disable whether communication can be established via any certificates.

Click the **[Submit]** button to apply a change. The change is only applied after the controller is restarted or after a BACnet restart.

“BACnet/SC Certificate Authority (CA)” Group

Table 138: WBM “BACnet Data Link” Page – “BACnet/SC Certificate Authority (CA)” Group

Parameters	Explanation
Chose file ...	Select the CA certificate on the computer for transfer to the device.
[Upload]	Transfer of the selected CA certificate to the device; after restart, this certificate is used as the CA certificate for BACnet/SC communication.

“BACnet/SC Certificate” Group

Table 139: WBM “BACnet Data Link” Page – “BACnet/SC Certificate” Group

Parameters	Explanation
Chose file ...	Select the device certificate on the computer for transfer to the device
[Upload]	Transfer of the selected device certificate to the device; After restart, this certificate is used for BACnet/SC communication.

“BACnet/SC Certificate Signing Request (CSR)” Group

Table 140: WBM “BACnet Configuration” Page – “BACnet/SC Certificate Signing Request (CSR)” Group

Parameters	Explanation
[Generate]	Generate a CSR and a new private key on the device.
[Download]	Download CSR from device.

“BACnet/SC Default Certificates” Group

Table 141: WBM “BACnet Data Link” Page – “BACnet/SC Default Certificates” Group

Parameters	Explanation
[Generate]	Generation of a new certificate

16.1.1.3.4 “BACnet Storage Location” Page

You can specify settings for saving of BACnet-specific parameters on this page.

Changes are applied without having to restart.

“BACnet Persistence” Group

This group lets you select the storage location (SD card/internal flash) for the persistence data.

If the persistence settings are changed, a pop-up window warns that data loss may occur until the next persistence is completed.

Table 142: WBM Page “BACnet Storage Location” – “BACnet Persistence” Group

Parameter	Meaning	
Storage location	You can select the storage location for the persistence data. Selection is possible only when both storage options are available.	
	Internal-Flash	Data will be stored in the controller's internal memory.
	SD-Card	Data will be stored on the SD card. If “SD card” has been selected and the card is no longer inserted, this option is no longer enabled and only the “internal flash” option can be selected.

“BACnet Trendlog” Group

This group lets you select the storage location (SD card/internal flash) for the trend log data.

Table 143: WBM Page “BACnet Storage Location” – “BACnet Trendlog” Group

Parameter	Meaning	
Storage location	You can select the storage location for the trend log data. Selection is possible only when both storage options are available.	
	Internal-Flash	Data will be stored in the controller's internal memory.
	SD-Card	Data will be stored on the SD card. If “SD card” has been selected and the card is no longer inserted, this option is no longer enabled and only the “internal flash” option can be selected.

“BACnet Eventlog” Group

This group lets you select the storage location (SD card/internal flash) for the event log data.

Table 144: WBM Page “BACnet Storage Location” – “BACnet Eventlog” Group

Parameter	Meaning	
Storage location	Select the storage location for the event log data here. Selection is possible only when both storage options are available.	
	Internal-Flash	Data will be stored in the controller's internal memory.
	SD-Card	Data will be stored on the SD card. If “SD card” has been selected and the card is no longer inserted, this option is no longer enabled and only the “internal flash” option can be selected.

16.1.1.4 “Security” Tab

16.1.1.4.1 “OpenVPN / IPsec Configuration” Page

The “OpenVPN / IPsec Configuration” page displays the settings for OpenVPN and IPsec.

“OpenVPN” Group

Table 145: WBM “OpenVPN / IPsec Configuration” Page – “OpenVPN” Group

Parameter	Explanation	
Current State	The current status of the OpenVPN service is displayed.	
	stopped	The service is disabled.
	running	The service is enabled.
OpenVPN enabled	Enable or disable the OpenVPN service.	
openvpn.config	Select an OpenVPN configuration file to be transferred from PC to product or vice versa.	

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

To select a file on the PC, click the **Choose file ...** selection field.

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

To transfer a file from product to PC, click the **[Download]** button.

The changes only take effect after the product restarts. For this purpose, use the WBM reboot function. Do not switch off the product too early!

“IPsec” Group

Table 146: WBM “OpenVPN / IPsec Configuration” Page – “IPsec” Group

Parameter	Explanation	
Current State	The current status of the IPsec service is displayed.	
	stopped	The service is disabled.
	running	The service is enabled.
IPsec enabled	Enable or disable the IPsec service.	
ipsec.conf	Select an IPsec configuration file to be transferred from PC to product or vice versa.	
ipsec.secrets	Select an IPsec configuration file to be transferred from PC to product or vice versa.	

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

To select a file on the PC, click the **Choose file ...** selection field.

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

To transfer a file from product to PC, click the **[Download]** button.

The changes only take effect after the product restarts. For this purpose, use the WBM reboot function. Do not switch off the product too early!

16.1.1.4.2 “General Firewall Configuration” Page

The “General Firewall Configuration” page displays the global firewall settings.

“Global Firewall Parameter” Group

Table 147: WBM “General Firewall Configuration” Page – “Global Firewall Parameter” Group

Parameter	Explanation
Firewall enabled entirely	Enables/disables the complete functionality of the firewall. This setting has the highest priority. If the firewall is disabled, all other settings have no direct effect. The configuration of the other parameters is possible nevertheless so that you can set the firewall parameters correctly before you enable the firewall. This setting is independent of the “Filter enabled” setting in the “MAC address filter state bridge <n>” group on the “MAC address filter state bridge <n>” page.
ICMP echo broadcast protection	Enable or disable the “ICMP echo broadcast” protection.
Max. UDP datagrams per second	Specify the maximum number of datagrams per second with the same source ports and the same destination ports between hosts.
Max. TCP connections per second	You can specify the maximum number of TCP connections per second.

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

16.1.1.4.3 “Interface Configuration” Page

The individual interfaces for the firewall settings are displayed on the “Interface Configuration” page.

“Firewall Configuration Bridge <n> / VPN / WAN” Group

A separate group is displayed for each configured bridge.

The settings in this group are based on the firewall configuration on the IP level.

Table 148: WBM "Interface Configuration" Page – "Firewall Configuration Bridge <n> / VPN / WAN" Group

Parameter	Explanation
Firewall enabled for Interface	Enable or disable the firewall for the respective bridge.
ICMP echo protection	Enable or disable the "ICMP echo" protection for the respective bridge. If you enable ICMP echo protection, all ICMP echo requests (pings) will be rejected and the ICMP echo limit per second and ICMP burst limit entries will be ineffective.
ICMP echo limit per second	You can specify the maximum number of "ICMP pings" per second. Input is only effective when ICMP echo protection is disabled. "0" = "Disabled"
ICMP burst limit (0 = disabled)	You can specify the maximum number of "ICMP echo bursts" per second. Input is only effective when ICMP echo protection is disabled. "0" = "Disabled"
Service Configuration	Enable or disable the firewall for the respective service.
FTP/FTPES	The services themselves must be enabled or disabled separately on the "Ports and Services" page.
FTPS (implicit)	
HTTP	
HTTPS	
I/O-CHECK	
PLC Runtime	
WebVisu – HTTP (port 8080)	
WebVisu – HTTPS (port 8081)	
SSH	
SNMP	
OPC UA (Port 4840)	
BACnet (Port 47808)	
DNP3 (port 20000)	
IEC60870-5-104 (port 2404)	
IEC61850 (port 102)	

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

The firewall ports listed in the following table are open by default on controllers with telecontrol functionality. The corresponding telecontrol services can be executed via these ports without the firewall blocking their communication.

Table 149: Ports for Telecontrol Functionality

Protocol	Port
DNP3	20000
IEC 60870-5-104	2404
IEC 61850	102

16.1.1.4.4 “Configuration of MAC Address Filter” Page

The “Configuration of MAC address filter” page displays the firewall configuration on the ETHERNET level.

The “MAC Address Filter Whitelist” contains two default entries with the following values:

Description:	All WAGO devices
MAC address:	00:30:DE:00:00:00
MAC mask:	ff:ff:ff:00:00:00

Description:	Enable docker bridges
MAC address:	02:42:00:00:00:00
MAC mask:	ff:ff:00:00:00:00

If you enable the first default entry, this already allows communication between different WAGO devices in the network.



Note

Enable the MAC address filter before activation!

Before activating the MAC address filter, you must enter and activate your own MAC address in the “MAC Address Filter Whitelist.”

Otherwise you cannot access the device via the ETHERNET. This also applies to other services that are used by your device, e.g., the IP configuration via DHCP. If the “MAC Address Filter Whitelist” does not contain the MAC address of your DHCP server, your device will lose its IP settings after the next refresh cycle and is then no longer accessible.

If the “MAC Address Filter Whitelist” does not contain an entry, the activation of the filter is prevented.

If at least one enabled address is entered, you will receive an appropriate warning before activation, which you have to acknowledge.

The check described above is only performed in the WBM but not in the CBM!

“Global MAC address filter state” Group

Table 150: WBM “Configuration of MAC Address Filter” Page – “Global MAC address filter state” Group

Parameters	Explanation
Filter enabled	Enable or disable the global MAC address filter.

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

“MAC address filter state Bridge <n>” Group

A separate group is displayed for each configured bridge.

Table 151: WBM “Configuration of MAC Address Filter” Page – “MAC address filter state Bridge <n>” Group

Parameter	Explanation
Filter enabled	Enable or disable here the MAC address filter for the specific bridge. This setting is independent of the “Firewall enabled entirely” setting on the General Firewall Configuration page.

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

“MAC address filter whitelist” Group

Each list entry has its own area in the display.

Table 152: WBM “Configuration of MAC Address Filter” Page – “MAC address filter whitelist” Group

Parameters	Explanation
Description	Description of the devices or areas that can be enabled by activating the filter when the firewall is generally enabled. The description is only visible for entries initially available in the factory default settings.
MAC address	Displays the MAC address of the relevant list entry.
MAC mask	This displays the MAC mask of the relevant list entry.
Filter enabled	Enable or disable the filter for the relevant list entry.
Add filter to whitelist	Create a new list entry.
MAC address	Enter here the MAC address for a new list entry. You can enter 10 filters.
MAC mask	Enter the MAC mask for the new list entry.
Filter enabled	Enable or disable the filter for the new list entry.

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

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

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

16.1.1.4.5 “Configuration of User Filter” Page

The “Configuration of User Filter” page displays the settings for custom firewall filters.

“User filter” Group

Each configured filter has its own area in the display.

Table 153: WBM “Configuration of User Filter” Page – “User Filter” Group

Parameters	Meaning	
Policy	This displays whether the network participant is permitted or excluded by the filter.	
Source IP address	The source IP address for the respective filter is displayed.	
Source Netmask	This displays the source netmask for the respective filter.	
Source Port	The source port number for the respective filter is displayed.	
Destination IP address	The destination IP address for the respective filter is displayed.	
Destination Netmask	The destination netmask for the respective filter is displayed.	
Destination Port	The destination port number for the respective filter is displayed.	
Protocol	The permitted protocols for the respective filter is displayed.	
Input interface	The permitted interfaces for the respective filter are displayed.	
Add new user filter	You can create up to 10 filters. You only have to enter values in the fields that are to be set for the filter. At least one value must be entered, all other fields can remain empty.	
Policy	Select here whether the network devices is to be allowed or excluded by the filter.	
	Allow	The network device is permitted.
	Drop	The network device is excluded.
Source IP address	Enter here the source IP address for the new filter.	
Source netmask	Enter here the source network mask for the new filter.	
Source port	Enter here the source port address for the new filter.	
Destination IP address	Enter here the destination IP address for the new filter.	
Destination subnet mask	Enter here the destination network mask for the new filter.	
Destination port	Enter here the destination port address for the new filter.	

Table 153: WBM "Configuration of User Filter" Page – "User Filter" Group

Parameters	Meaning	
Protocol	Enter here the protocols for the new filter.	
	TCP/ UDP	The TCP service and UDP service are filtered.
	TCP	The TCP service is filtered.
	UDP	The UDP service is filtered.
Input interface	Enter here the interfaces for the new filter.	
	Any	All interfaces are filtered.
	Bridge <n>	The interfaces assigned for bridge <n> are filtered. Only the configured bridges are displayed.
	VPN	The VPN interface is filtered.

Click **[Add]** to apply the new filter. The change takes effect immediately.

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

16.1.1.4.6 “Certificates” Page

On the “Certificates” page, you will find options to install or delete certificates and keys.

“Installed Certificates” Group

Table 154: WBM “Certificates” Page – “Certificate List” Group

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

To select a file on the PC, click the **Choose file ...** selection field.

To transfer the selected file PC to the product, click the **[Upload]** button. The changes take effect immediately.

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

Click **[Delete]** to delete an entry. The changes take effect immediately.

“Installed Private Keys” Group

Table 155: WBM “Certificates” Page – “Private Key List” Group

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

To select a file on the PC, click the **Choose file ...** selection field.

To transfer the selected file PC to the product, click the **[Upload]** button. The changes take effect immediately.

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

Click **[Delete]** to delete an entry. The changes take effect immediately.

16.1.1.4.7 “Boot mode configuration” Page

See the “Boot mode configuration” page for boot option settings.

“Force internal boot” Group

Table 156: WBM Page “Boot mode configuration” – “Force internal boot” Group

Parameter	Meaning	
Boot mode	You set the boot option for the product.	
	Memory card or internal flash	You can boot from the internal flash or from the memory card.
	Internal flash only	You can only boot from the internal flash.



Note

If you force booting from the internal flash, the device can no longer be booted from the memory card!

If a connection via ETHERNET is no longer possible due to problems or incorrect configuration, you have the option of making the product accessible again via the service interface and “WAGO Ethernet Settings”.

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

16.1.1.4.8 “Security Settings” Page

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

“TLS Configuration” Group

Table 157: “Security Settings” WBM Page – “TLS Configuration” Group

Parameters	Explanation	
TLS Configuration	You can set what TLS versions and cryptographic methods are allowed for HTTPS.	
	Standard	The Webserver allows TLS 1.0, TLS 1.1, TLS 1.2 and TLS 1.3, as well as cryptographic methods that are no longer considered secure.
	Strong	The Webserver only allows TLS Version 1.2 and 1.3 and strong algorithms. Older software and older operating systems may not support TLS 1.2 and TLS 1.3.

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

Note**BSI TR-02102 Technical Guidelines**

The rules for the “Strong” setting are based on the TR-02102 technical guidelines of the German Federal Office for Information Security (BSI).

You can find the guidelines on the Internet at: <https://www.bsi.bund.de> > “Publications” > “Technical Guidelines.”

16.1.1.4.9 “Advanced Intrusion Detection Environment (AIDE)” Page

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

“Run AIDE check at startup” Group

Table 158: WBM “Advanced Intrusion Detection Environment (AIDE)” Page – “Run AIDE check at startup” Group

Parameter	Explanation
Service active	Here, you can activate/deactivate the “AIDE check” when the controller is started.

Click the **[Submit]** button to apply the changes. The changes only take effect when the controller restarts.

“Refresh Options” group

Table 159: WBM “Advanced Intrusion Detection Environment (AIDE)” Page – “Control AIDE and show log” Group

Parameter	Explanation
Select Action	Select here the action to be executed.
	readlog The log data are displayed.
	init The database is initialized and filled with the current values.
	check The current values are compared against the values stored in the database.
	update The current values are compared with the values stored in the database and the database then updated.
Read only the last n	Activate display of only the last n messages. You also specify the number of messages to be displayed.
Automatic refresh interval (sec)	Select the checkbox to enable cyclic refresh. Enter the cycle time in seconds in which a cyclic refresh is performed. The label of the button (“Refresh”/“Start”/“Stop”) changes depending on status.

Click **[Refresh]** to update the display. The button is only displayed if the cyclic refresh is not enabled.

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

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

The cyclical refresh is performed for as long as the “Advanced Intrusion Detection Environment (AIDE)” page is open. If you change the WBM page, the

update is stopped until you call up the “Advanced Intrusion Detection Environment (AIDE)” page again.

The messages are displayed below the settings.

16.1.1.4.10 “WAGO Device Access” Page

On the “WAGO Device Access” page you will find settings for authentication when scanning the node.



Note

Beta Status

In the present firmware version, the “WAGO Device Access” functionality is still in beta!

“Unauthenticated Requests” Group

Table 160: WBM Page “WAGO Device Access” – “Unauthenticated Requests” Group

Parameter	Meaning
Allow unauthenticated Device Scan	You set whether the node can be scanned without authentication. In the default setting, authentication is switched off. To increase the security level, you can enforce authentication for node scanning. In the current beta status, only head stations but no I/O modules are recognized when scanning!

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

16.1.1.5 “Diagnostic” Tab

16.1.1.5.1 “Log Message Viewer” Page

The settings for displaying diagnostic messages are shown on the “Log Message Viewer” page.

“Refresh Options” Group

Table 161: WBM “Log Message Viewer” Page – “Refresh Options” Group

Parameters	Meaning	
Read only the last	Activate display of only the last n messages. You also specify the number of messages to be displayed.	
Automatic refresh interval (sec)	Select the checkbox to enable cyclic refresh. Enter the cycle time in seconds in which a cyclic refresh is performed. The label of the button (“Refresh”/“Start”/“Stop”) changes depending on status.	
Source	Select the source of the diagnostic messages. The drop-down list depends on the user who is logged in.	
	user	Default diagnostic messages only
	admin	Default diagnostic messages and all log files in the folder <code>/var/log/*</code>

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

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

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

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

The messages are displayed below the settings.

16.1.1.5.2 “Download” Page

“Diagnostic Information” Group

Click the **[Download]** button to download diagnostic information from the device. An archive file is then created that contains the log messages, the firmware version and a list of the installed packages. This file is saved to the Downloads folder on your computer.

16.1.1.5.3 “Network Capture” Page

All the settings required for logging the network traffic on the device and downloading these logs are available on the “Network Capture” page. The current status of network traffic logging is displayed.

“State” Group

Table 162: “Network Capture” Page – “State” Group

Parameter	Explanation
Current State	The current status of network traffic logging is displayed here.
Last Captured Package Count	Network packages already logged are displayed here.
Last Refresh Time	The last refresh time for Current State and Last Captured Package Count is displayed here.

“Configuration” Group

Table 163: “Network Capture” Page – “Configuration” Group

Parameter	Explanation	
Enable	Here, you can activate or deactivate logging.	
Rotate Log Files	<p>Here, you can activate or deactivate rotating logging.</p> <p>When this option is activated, network traffic is recorded in up to three files of the set maximum file size.</p> <p>When the maximum file size for the first file is reached, the data is logged in a second file and then to a third file when the second file is full. When the maximum size of the third file is reached, the data in the first file is then overwritten.</p>	
Max. Filesize	Specify the maximum file size for the data log file.	
Storage Location	Select the storage location for the logged data. Selection is possible only when both storage options are available.	
	Internal Flash	Data will be stored in the controller's internal memory.
	SD Card	Data will be stored on the SD card. If “SD card” has been selected and the card is no longer inserted, this option is no longer enabled and only the “Internal flash” option can be selected.
Listen On Network Interface	<p>Here, select the network interface from which network traffic is to be logged.</p> <p>Any of the available network interfaces of the device can be selected.</p>	

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

“Filter Configuration” Group

Table 164: “Network Capture” Page – “Filter Configuration” Group

Parameter	Explanation
Capture Filter	You can set capture filters here. These filters are used to log only the relevant or required data traffic. This enables you to record only the communication for one port, for example, or only from a defined IP address. More information on possible filter settings is given in the “Capture Filter” notes in the “Wireshark” documentation.

Click the **[Check]** button to check the specified “Capture Filter” for correctness.

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

“Log Download” Group

Table 165: “Network Capture” Page – “Log Download” Group

Parameter	Explanation
Select Log File	Select a log here that can be downloaded using the [Download] button.

Click the **[Download]** button to download the selected log from the device.

Click the **[Download All]** button to download all the logs from the device.

List of Figures

Figure 1: View	25
Figure 2: Labeling (Example)	28
Figure 3: Type plate (Example)	28
Figure 4: RS-485 Bus Termination	33
Figure 5: CANopen Standard Bus Termination.....	35
Figure 6: Schematic diagram.....	40
Figure 7: Example of Interface Assignment via WBM	50
Figure 8: One Bridge with Two Ports	52
Figure 9: Two Bridges with One/One Ports	52
Figure 10: Connecting the Controller to a Cloud Service (Example)	65
Figure 11: Spacing	78
Figure 12: Insert Controller.....	79
Figure 13: Removing the Female Connector without Wiring (Application Example)	80
Figure 14: Removing the Female Connector with Wiring (Application Example).80	
Figure 15: "WAGO Ethernet Settings" – Starting Screen (Example)	88
Figure 16: "WAGO Ethernet Settings" – "Network" Tab (Example)	89
Figure 17: "Open DHCP", Example Figure	92
Figure 18: Example of a Function Test	93
Figure 19: Entering Authentication	99
Figure 20: Password Reminder	101
Figure 21: WBM Browser Window (Example).....	104
Figure 22: WBM Header with Tabs that Cannot be Displayed (Example)	104
Figure 23: WBM Status Bar (Example).....	105
Figure 24: "WAGO Ethernet Settings" – Start Screen (Example).....	106
Figure 25: "WAGO Ethernet Settings" – Communication Link (Example)	107
Figure 26: "WAGO Ethernet Settings" – Identification Tab (Example)	108
Figure 27: "WAGO Ethernet Settings" – Network Tab (Example)	109
Figure 28: "WAGO Ethernet Settings" – Protocol Tab (Example)	111
Figure 29: "WAGO Ethernet Settings" – Status Tab (Example)	112
Figure 30: Correlation Between "IEC 61131-3" Variables and PFC Variables ..	130

List of Tables

Table 1: Number Notation	14
Table 2: Font Conventions	14
Table 3: Legend for figure "View"	26
Table 4: Labeling and type plate	27
Table 5: Network Connections ETHERNET – "X1", "X2"	29
Table 6: Supply Voltage – "X4"	29
Table 7: Digital inputs – "X12"	30
Table 8: Digital outputs – "X5"	31
Table 9: Analog inputs – "X14"	31
Table 10: Analog outputs – "X6"	32
Table 11: Communication Interface RS-485 – "X11"	32
Table 12: CANopen Interface Pin Assignment – X8	34
Table 13: Analog Temperature Sensors – "X13"	36
Table 14: System LEDs	37
Table 15: "LNK ACT" LEDs	37
Table 16: Memory Card Slot LED	37
Table 17: Status DI/DO LEDs	37
Table 18: CAN LED Indicator	37
Table 19: Mode Selector Switch	38
Table 20: Technical Data – Mechanical Data	41
Table 21: Technical Data – System Data	41
Table 22: Technical Data – Power Supply	42
Table 23: Technical Data – Clock	42
Table 24: Technical Data – Programming	43
Table 25: Technical Data – ETHERNET	43
Table 26: Technical Data – CANopen	44
Table 27: Technical Data – Communication Interface	44
Table 28: Technical Data – Field Wiring	45
Table 29: Technical Data – Digital Inputs	45
Table 30: Technical Data – Digital Outputs	46
Table 31: Technical Data – Analog Inputs	46
Table 32: Technical Data – Analog Outputs	46
Table 33: Technical Data – Climatic Environmental Conditions	47
Table 34: Technical Data – Analog Temperature Sensors	48
Table 35: Technical Data – Fieldbus	48
Table 36: Technical Data – Other	48
Table 37: MAC ID and IP Address Assignment for One Bridge with Two Ports ..	52
Table 38: MAC ID and IP Address Assignment for Two Bridges with One/One Ports	52
Table 39: WBM Users	54
Table 40: Linux® Users	54
Table 41: List of Parameters Transmitted via DHCP	63
Table 42: Components of the Cloud Connectivity Software Package	66
Table 43: Loading a Boot Project	73
Table 44: Installation positions and permitted ambient temperatures	74
Table 45: WAGO DIN Rails	77
Table 46: Legend for Figures "Removing the Female Connector ..."	80

Table 47: Default IP Addresses for ETHERNET Interfaces	86
Table 48: Network Mask 255.255.255.0	86
Table 49: User Settings in the Default State	101
Table 50: Access Rights for WBM Pages	102
Table 51: CODESYS V3 Priorities	114
Table 52: Process Image – Analog Inputs	117
Table 53: Process Image – Analog Outputs	117
Table 54: Process Image – Analog Temperature Inputs	118
Table 55: Process Image – Digital Inputs	118
Table 56: Process Image – Digital Outputs	119
Table 57: Overview of Addresses in the Object Directory	120
Table 58: Indexing of “IEC 61131-3” Variable Data in the Object Directory	128
Table 59: Fieldbus Access to PFC Output Data	129
Table 60: Examples for CODESYS Access to PFC Variables	131
Table 61: Maximum Indices and Sub-Indices for “IEC 61131-3” Variables	132
Table 62: Example of “IEC 61131-3” Output Variables	133
Table 63: Diagnostics via SYS LED	136
Table 64: RUN LED Diagnostics	136
Table 65: Diagnostics CAN LED	138
Table 66: “LNK ACT” LED Diagnostics	139
Table 67: Diagnostics via Memory Card Slot LED	139
Table 68: Accessories – Tools	148
Table 69: WBM “Device Status” Page – “Device Details” Group	149
Table 70: WBM “Device Status” Page – “Network TCP/IP Details” Group	150
Table 71: WBM “PLC Runtime Information” Page – “Runtime” Group	152
Table 72: WBM “PLC Runtime Configuration” Page – “General PLC Runtime Configuration” Group	158
Table 73: WBM “PLC Runtime Configuration” Page – “Webserver Configuration” Group	159
Table 74: WBM “TCP/IP Configuration” Page – “TCP/IP Configuration” Group	160
Table 75: WBM “TCP/IP Configuration” Page – “DNS Server” Group	161
Table 76: WBM “Ethernet Configuration” Page – “Bridge Configuration” Group	162
Table 77: WBM “Ethernet Configuration” Page – “Switch Configuration” Group	163
Table 78: WBM “Ethernet Configuration” Page – “Dummy Interfaces” Group	164
Table 79: WBM “Ethernet Configuration” Page – “VLAN Interfaces” Group	164
Table 80: WBM “Ethernet Configuration” Page – “Ethernet Interface Configuration” Group	165
Table 81: WBM “Configuration of Host and Domain Name” Page – “Hostname” Group	166
Table 82: WBM “Configuration of Host and Domain Name” Page – “Domain Name” Group	166
Table 83: WBM “Routing” Page – “IP Forwarding through multiple interfaces” Group	168
Table 84: WBM “Routing” Page – “Custom Routes” Group	169
Table 85: WBM “Routing” Page – “IP-Masquerading” Group	171
Table 86: WBM “Routing” Page – “Port Forwarding” Group	172
Table 87: WBM “Spanning Tree Protocol” Page – “Status” Group	173
Table 88: WBM “Spanning Tree Protocol” Page – “Parameter Settings” Group	174

Table 89: WBM "Clock Settings" Page – "Timezone and Format" Group.....	176
Table 90: WBM "Clock Settings" Page – "UTC Time and Date" Group.....	176
Table 91: WBM "Clock Settings" Page – "Local Time and Date" Group.....	177
Table 92: WBM "Create Bootable Image" Page – "Create bootable image from active partition" Group.....	178
Table 93: WBM "Firmware Backup" Page – "Firmware Backup" Group.....	179
Table 94: WBM "Firmware Restore" Page – "Firmware Restore" Group.....	181
Table 95: WBM "Active System" Page – "Boot Device" Group	183
Table 96: WBM "Active System" Page – "System <n> (Internal Flash)" Group ..	183
Table 97: WBM "Mass Storage" Page – "Devices" Group	184
Table 98: WBM "Mass Storage" Page – "Create new Filesystem on Memory Card" Group	184
Table 99: WBM "Software Uploads" Page – "Upload New Software" Group.....	185
Table 100: WBM "Configuration of Network Services" Page – "FTP" Group.....	186
Table 101: WBM "Configuration of Network Services" Page – "FTPES (explicit FTPS)" Group	186
Table 102: WBM "Configuration of Network Services" Page – "HTTP" Group ..	187
Table 103: WBM "Configuration of Network Services" Page – "HTTPS" Group ..	187
Table 104: WBM "Configuration of Network Services" Page – "I/O-CHECK" Group.....	187
Table 105: WBM "Configuration of NTP Client" Page – "NTP Client Configuration" Group.....	188
Table 106: WBM "PLC Runtime Services" Page – "CODESYS V3" Group.....	189
Table 107: WBM "SSH Server Settings" Page – "SSH Server" Group.....	190
Table 108: WBM "DHCP Server Configuration" Page – "DHCP Configuration Bridge <n>" Group	191
Table 109: WBM "Configuration of DNS Server" Page – "DNS Server" Group ..	192
Table 110: WBM "Status Overview" Page – "Connection <n>" Group	193
Table 111: WBM "Configuration of Connection <n>" Page – "Configuration" Group.....	194
Table 112: Display of the Selection and Input Fields Depending on the Selected Cloud Platform	196
Table 113: Choice of Data Protocol Depending on the Selected Cloud Platform	199
Table 114: Display of the Selection and Input Fields Depending on the Selected Data Protocol	199
Table 115: Choice of Cache Mode Depending on the Selected Data Protocol ..	199
Table 116: Display of the Selection and Input Fields Depending on the Selected Authentication	200
Table 117: WBM "Configuration of General SNMP Parameters" Page – "General SNMP Configuration" Group	201
Table 118: WBM "Configuration of SNMP v1/v2c Parameters" Page – "Communities" Group.....	202
Table 119: WBM "Configuration of SNMP v1/v2c Parameters" Page – "Trap Receivers" Group.....	203
Table 120: WBM "Configuration of SNMP v3 Parameters" Page – "Users" Group	204
Table 121: WBM "Configuration of SNMP v3 Parameters" Page – "Trap Receivers" Group.....	206
Table 122: WBM "Commissioning Settings" Page – "Commissioning" Group...	208

Table 123: WBM Page “Dockert Settings” – group “Dockert Status”	209
Table 124: WBM “WBM User Configuration” Page – “Change Password” Group	210
Table 125: WBM “OPC UA Configuration” Page – “OPC UA Server Configuration” Group	211
Table 126: WBM “OPC UA Configuration” Page – “OPC UA Server Security Settings” Group	212
Table 127: WBM “BACnet Status” Page – “BACnet Information” Group	213
Table 128: WBM “BACnet Status” Page – “BACnet License” Group	213
Table 129: WBM “BACnet Status” Page – “BACnet Data Link” Group	213
Table 130: WBM “BACnet Data Link” Page – “BACnet Restart” Group	214
Table 131: WBM “BACnet Configuration” Page – “BACnet Service” Group	214
Table 132: WBM “BACnet Configuration” Page – “BACnet Data” Group	214
Table 133: WBM “BACnet Configuration” Page – “BACnet Log Level” Group ..	215
Table 134: WBM “BACnet Configuration” Page – “BACnet Network Capture” Group	215
Table 135: WBM “BACnet Data Link” Page – “BACnet Restart” Group	216
Table 136: WBM “BACnet Data Link” Page – “BACnet/IP” Group	216
Table 137: WBM “BACnet Data Link” Page – “BACnet/SC” Group	216
Table 138: WBM “BACnet Data Link” Page – “BACnet/SC Certificate Authority (CA)” Group	217
Table 139: WBM “BACnet Data Link” Page – “BACnet/SC Certificate” Group ..	217
Table 140: WBM “BACnet Configuration” Page – “BACnet/SC Certificate Signing Request (CSR)” Group	217
Table 141: WBM “BACnet Data Link” Page – “BACnet/SC Default Certificates” Group	217
Table 142: WBM Page “BACnet Storage Location” – “BACnet Persistence” Group	218
Table 143: WBM Page “BACnet Storage Location” – “BACnet Trendlog” Group	218
Table 144: WBM Page “BACnet Storage Location” – “BACnet Eventlog” Group	219
Table 145: WBM “OpenVPN / IPsec Configuration” Page – “OpenVPN” Group	220
Table 146: WBM “OpenVPN / IPsec Configuration” Page – “IPsec” Group	221
Table 147: WBM “General Firewall Configuration” Page – “Global Firewall Parameter” Group	222
Table 148: WBM “Interface Configuration” Page – “Firewall Configuration Bridge <n> / VPN / WAN” Group	224
Table 149: Ports for Telecontrol Functionality	225
Table 150: WBM “Configuration of MAC Address Filter” Page – “Global MAC address filter state” Group	226
Table 151: WBM “Configuration of MAC Address Filter” Page – “MAC address filter state Bridge <n>” Group	227
Table 152: WBM “Configuration of MAC Address Filter” Page – “MAC address filter whitelist” Group	227
Table 153: WBM “Configuration of User Filter” Page – “User Filter” Group	228
Table 154: WBM “Certificates” Page – “Certificate List” Group	230
Table 155: WBM “Certificates” Page – “Private Key List” Group	230

Table 156: WBM Page “Boot mode configuration” – “Force internal boot” Group	231
Table 157: “Security Settings” WBM Page – “TLS Configuration” Group	232
Table 158: WBM “Advanced Intrusion Detection Environment (AIDE)” Page – “Run AIDE check at startup” Group	233
Table 159: WBM “Advanced Intrusion Detection Environment (AIDE)” Page – “Control AIDE and show log” Group	233
Table 160: WBM Page “WAGO Device Access” – “Unauthenticated Requests” Group	235
Table 161: WBM “Log Message Viewer” Page – “Refresh Options” Group	236
Table 162: “Network Capture” Page – “State” Group	238
Table 163: “Network Capture” Page – “Configuration” Group	239
Table 164: “Network Capture” Page – “Filter Configuration” Group	240
Table 165: “Network Capture” Page – “Log Download” Group	240



WAGO GmbH & Co. KG

Postfach 2880 • D - 32385 Minden

Hansastraße 27 • D - 32423 Minden

Phone: +49 571 887 – 0

Fax: +49 571 887 – 844169

E-Mail: info@wago.com

Internet: www.wago.com