

# WAGO I/O System 750/753

Controller PFC100 2. Generation, PFC200 2. Generation und PFC300

750-811x, 750-821x, 750-8302



© 2025 WAGO GmbH & Co. KG  
Alle Rechte vorbehalten.

**WAGO GmbH & Co. KG**

Hansastraße 27  
D - 32423 Minden

Tel: +49 (0) 571/887 – 0  
E-Mail: ✉ [info@wago.com](mailto:info@wago.com)  
Web: 🌐 [www.wago.com](http://www.wago.com)

**Technischer Support**

Tel: +49 (0) 571/887 – 44555  
E-Mail: ✉ [support@wago.com](mailto:support@wago.com)  
Web: 🌐 [www.wago.com/support](http://www.wago.com/support)

Es wurden alle erdenklichen Maßnahmen getroffen, um die Richtigkeit und Vollständigkeit der vorliegenden Dokumentation zu gewährleisten. Da sich trotz aller Sorgfalt Fehler nicht vollständig vermeiden lassen, sind wir für Hinweise und Anregungen jederzeit dankbar.

E-Mail: ✉ [documentation@wago.com](mailto:documentation@wago.com)

Wir weisen darauf hin, dass die in dieser Dokumentation verwendeten Soft- und Hardwarebezeichnungen und Markennamen der jeweiligen Firmen im Allgemeinen einem Warenzeichenschutz, Markenzeichenschutz oder patentrechtlichem Schutz unterliegen.

**WAGO ist eine eingetragene Marke der WAGO Verwaltungsgesellschaft mbH.**

# Inhaltsverzeichnis

<b>1 Bestimmungen.....</b>	<b>7</b>
1.1 Gültigkeitsbereich.....	7
<b>2 Überblick .....</b>	<b>12</b>
<b>3 Funktionen .....</b>	<b>13</b>
3.1 Funktionsübersicht.....	13
3.2 Systemfunktionen.....	14
3.2.1 Produkt- und Systemstatus.....	14
3.2.2 Echtzeituhr.....	15
3.2.2.1 Anzeige/Manuelle Einstellung.....	15
3.2.2.2 Automatische Einstellung.....	15
3.2.3 Laufzeitumgebung CODESYS V3.....	16
3.2.3.1 Speicherbereiche unter CODESYS V3.....	16
3.2.3.1.1 Programm- und Datenspeicher.....	16
3.2.3.1.2 Bausteinbegrenzung.....	16
3.2.3.1.3 Merkerbereich (Memory) und Retain-Bereich.....	16
3.2.3.2 CODESYS V3-Prioritäten.....	17
3.2.3.3 CODESYS V3-Dienst- und Porteinstellungen.....	17
3.3 Hardwarefunktionen.....	19
3.3.1 Adresswahlschalter.....	19
3.3.2 Betriebsartenschalter/Reset-Taster.....	19
3.3.2.1 Betriebsartenschalter/Reset-Taster aktivieren/deaktivieren.....	19
3.3.2.2 Temporär feste IP-Adressen einstellen.....	19
3.3.2.3 Software-Reset (Neustart).....	20
3.3.2.4 Controller-Reset.....	20
3.3.3 Kommunikationsschnittstelle.....	21
3.3.3.1 PFC100/PFC200.....	21
3.3.3.2 PFC300.....	22
3.3.4 Service-Schnittstelle.....	23
3.4 Konfigurationsfunktionen.....	24
3.4.1 Web-based Management (WBM).....	24
3.5 Netzwerkfunktionen.....	25
3.5.1 Netzwerkkonfiguration.....	25
3.5.1.1 Schnittstellenkonfiguration.....	25
3.5.1.1.1 Bridge-Konfiguration.....	25
3.5.1.1.2 Dummy-Interfaces.....	25
3.5.1.1.3 VLAN-Interfaces.....	25
3.5.1.1.4 Port Mirror-Konfiguration (PFC100 G2, PFC200 G2 - 2-Port, PFC300).....	25
3.5.1.1.5 Storm Control-Konfiguration (PFC100 G2, PFC200 G2 - 2-Port).....	26
3.5.1.1.6 Storm Control-Konfiguration (PFC200 G2 - 4-Port).....	26
3.5.1.1.7 Storm Control-Konfiguration (PFC300).....	26
3.5.1.1.8 Ethernet Interface-Konfiguration (PFC100 G2, PFC200 G2 - 2-Port).....	26
3.5.1.1.9 Ethernet Interface-Konfiguration (PFC200 G2 - 4-Port, PFC300).....	27
3.5.1.2 TCP/IP-Konfiguration.....	27
3.5.1.2.1 Bridge-Interfaces.....	27
3.5.1.2.2 Dummy-Interfaces.....	28
3.5.1.2.3 VLAN-Interfaces.....	28
3.5.1.2.4 DNS-Server.....	28
3.5.1.3 Hostname/Domainname.....	29
3.5.1.3.1 Hostname.....	29

3.5.1.3.2	Domainname.....	29
3.5.1.4	Routing .....	30
3.5.1.4.1	Statische Routen .....	31
3.5.1.4.2	Dynamische Routen .....	33
3.5.1.4.3	IP-Masquerading.....	34
3.5.1.4.4	Port-Forwarding .....	34
3.5.2	Netzwerksicherheit.....	35
3.5.2.1	Benutzer und Passwörter .....	35
3.5.2.2	Webserverauthentifizierung.....	36
3.5.2.2.1	TLS-Verschlüsselung .....	37
3.5.2.3	Root-Zertifikate .....	37
3.5.2.4	Firewall.....	38
3.5.2.4.1	Globale Firewall-Einstellungen .....	38
3.5.2.4.2	Schnittstellenbezogene Firewall-Einstellungen.....	38
3.5.2.4.3	MAC-Adressenfilter.....	39
3.5.2.4.4	User-Filter .....	40
3.5.3	Netzwerkdienste.....	41
3.5.3.1	DHCP-Client .....	41
3.5.3.2	DHCP-Server .....	41
3.5.3.3	DNS-Server .....	43
3.5.3.4	SNMP .....	43
3.5.3.4.1	SNMP v1/v2c .....	44
3.5.3.4.2	SNMP v3.....	45
3.5.3.5	FTP/FTPES .....	46
3.5.3.6	HTTP/HTTPS.....	47
3.5.3.7	I/O-CHECK .....	47
3.5.3.8	SSH-Server.....	48
3.5.3.9	Docker®.....	48
3.6	Cloud-Connectivity.....	48
3.7	Feldbusfunktionen .....	53
3.7.1	OPC UA .....	53
3.7.2	BACnet .....	55
3.7.3	CANopen-Master und -Slave .....	59
3.7.3.1	Objektverzeichnis .....	60
3.7.3.2	Kommunikationsprofil.....	60
3.7.3.2.1	Masterkonfiguration .....	63
3.7.3.3	Datenaustausch.....	64
3.7.3.3.1	Kommunikationsobjekte des Controllers .....	65
3.7.3.3.2	Feldbuspezifische Adressierung.....	65
3.7.3.3.3	Beispiele für die Definition von PFC-Feldbusvariablen.....	67
3.7.3.3.4	Verwendung des CANopen Slave (Device) unter CODESYS V3 .....	68
3.7.3.3.5	Verwendung als CAN Layer 2 Gerät .....	68
3.7.3.3.5	Verwendung als CAN Layer 2 Gerät .....	68
3.8	Speicherfunktionen.....	69
3.8.1	Datensicherung.....	69
3.8.1.1	Backup-Funktion .....	69
3.8.1.2	Restore-Funktion.....	71
3.8.2	Speicherkartenfunktion.....	73
3.8.2.1	Einfügen einer Speicherkarte im Betrieb.....	73
3.8.2.2	Entfernen der Speicherkarte im Betrieb.....	73
3.8.2.3	Einstellung des Home-Verzeichnisses für das Laufsystem .....	73
3.8.2.4	Boot-Projekt laden .....	74
3.9	Diagnosefunktionen .....	74
3.9.1	Diagnose über Anzeigeelemente .....	74
3.9.1.1	Diagnose über Blinksequenzen.....	75
3.9.1.1.1	Fehlercodes der I/O-LED .....	75
3.9.1.1.2	Fehlercodes der MS-LED .....	79
3.9.2	Diagnose über WBM.....	79

<b>4</b>	<b>In Betrieb nehmen .....</b>	<b>81</b>
4.1	Einschalten des Controllers .....	81
4.2	Ermitteln der IP-Adresse des Host-PC .....	81
4.3	Einstellen einer IP-Adresse.....	82
4.3.1	IP-Verbindung über USB (PFC300).....	82
4.3.2	Einstellen einer IP-Adresse über das WBM .....	82
4.3.3	Zuweisen einer IP-Adresse mit DHCP .....	83
4.3.4	Ändern einer IP-Adresse mit "WAGO Ethernet Settings".....	83
4.3.5	IP-Adressvorgabe mit Adresswahlschalter einstellen.....	84
4.3.6	Temporär feste IP-Adressen einstellen .....	86
4.4	Testen der Netzwerkverbindung.....	87
4.5	Passwörter ändern.....	87
4.6	Ausschalten/Neustart.....	88
<b>5</b>	<b>Konfigurieren.....</b>	<b>89</b>
5.1	Konfigurieren im WBM.....	89
5.1.1	Allgemeine Seiteninformationen.....	90
5.1.2	WBM-Seitenübersicht und Zugriffsrechte.....	91
5.2	Konfigurieren mit „WAGO Ethernet Settings“ .....	93
5.2.1	Registerkarte Identifikation.....	94
5.2.2	Registerkarte Netzwerk.....	95
5.2.3	Registerkarte SPS.....	96
5.2.4	Registerkarte Status.....	96
<b>6</b>	<b>Service .....</b>	<b>98</b>
6.1	Firmwareänderungen .....	98
6.1.1	Firmware-Update/-Downgrade mit WAGOupload durchführen.....	98
6.1.2	Firmware-Update/-Downgrade mit Speicherkarte und WBM durchführen..	99
6.2	Reset-Funktionen auslösen .....	99
6.2.1	Warmstart-Reset .....	99
6.2.2	Kaltstart-Reset .....	100
6.2.3	Software-Reset (Neustart).....	100
6.2.4	Controller-Reset.....	100
6.3	Root-Zertifikate aktualisieren .....	101
<b>7</b>	<b>Anhang.....</b>	<b>102</b>
7.1	Konfigurationsdialoge .....	102
7.1.1	WBM-Seiten .....	102
7.1.1.1	WBM-Seitenübersicht und Zugriffsrechte .....	102
7.1.1.2	Registerkarte „Information“ .....	103
7.1.1.2.1	Seite „Device Status“ .....	103
7.1.1.2.2	Seite „Vendor Information“ .....	104
7.1.1.2.3	Seite „PLC Runtime Information“ .....	105
7.1.1.2.4	Seite „WAGO Software License Agreement“ .....	105
7.1.1.2.5	Seite „Open Source Licenses“ .....	105
7.1.1.2.6	Seite „WBM Third Party License Information“ .....	105
7.1.1.2.7	Seite „Trademarks Information“ .....	105
7.1.1.2.8	Seite „WBM Version“ .....	105
7.1.1.3	Registerkarte „Configuration“ .....	105
7.1.1.3.1	Seite „PLC Runtime Configuration“ .....	105
7.1.1.3.2	Seite „TCP/IP Configuration“ .....	107
7.1.1.3.3	Seite „Ethernet Configuration“ .....	109
7.1.1.3.4	Seite „Configuration of Host and Domain Name“ .....	111
7.1.1.3.5	Seite „Routing“ .....	112
7.1.1.3.6	Seite „Spanning Tree Protocol“ .....	114
7.1.1.3.7	Seite „Clock Settings“ .....	117

7.1.1.3.8	Seite „Configuration of Serial Interface“ .....	117
7.1.1.3.9	Seite „Configuration of Service Interface“ .....	119
7.1.1.3.10	Seite „Create bootable Image“ .....	120
7.1.1.3.11	Seite „Firmware Backup“ .....	120
7.1.1.3.12	Seite „Firmware Restore“ .....	122
7.1.1.3.13	Seite „Active System“ .....	123
7.1.1.3.14	Seite „Mass Storage“ .....	124
7.1.1.3.15	Seite „Software Uploads“ .....	125
7.1.1.3.16	Seite „Configuration of Network Services“ .....	125
7.1.1.3.17	Seite „Configuration of NTP Client“ .....	127
7.1.1.3.18	Seite „PLC Runtime Services“ .....	127
7.1.1.3.19	Seite „SSH Server Settings“ .....	128
7.1.1.3.20	Seite „DHCP Server Configuration“ .....	128
7.1.1.3.21	Seite „Configuration of DNS Server“ .....	129
7.1.1.3.22	Seite „Status overview“ .....	129
7.1.1.3.23	Seite „Configuration of Connection <n>“ .....	130
7.1.1.3.24	Seite „Controls Settings“ .....	133
7.1.1.3.25	Seite „Configuration of general SNMP parameters“ .....	134
7.1.1.3.26	Seite „Configuration of SNMP v1/v2c Parameters“ .....	134
7.1.1.3.27	Seite „Configuration of SNMP v3 Parameters“ .....	135
7.1.1.3.28	Seite „Commissioning Settings“ .....	136
7.1.1.3.29	Seite „Docke Settings“ .....	137
7.1.1.3.30	Seite „WBM User Configuration“ .....	137
7.1.1.4	Registerkarte „Fieldbus“ .....	138
7.1.1.4.1	Seite „OPC UA Configuration“ .....	138
7.1.1.4.2	Seite „BACnet Status“ .....	139
7.1.1.4.3	Seite „BACnet Configuration“ .....	140
7.1.1.4.4	Seite „BACnet Data Link“ .....	142
7.1.1.4.5	Seite „BACnet Storage Location“ .....	143
7.1.1.4.6	Seite „BACnet Info“ .....	144
7.1.1.5	Registerkarte „Security“ .....	145
7.1.1.5.1	Seite „OpenVPN / IPsec“ .....	145
7.1.1.5.2	Seite „General Firewall Configuration“ .....	146
7.1.1.5.3	Seite „Interface Configuration“ .....	147
7.1.1.5.4	Seite „Configuration of MAC address filter“ .....	148
7.1.1.5.5	Seite „Configuration of User Filter“ .....	149
7.1.1.5.6	Seite „Certificates“ .....	150
7.1.1.5.7	Seite „Boot Mode Configuration“ .....	150
7.1.1.5.8	Seite „Security Settings“ .....	151
7.1.1.5.9	Seite „Advanced Intrusion Detection Environment (AIDE)“ ....	151
7.1.1.5.10	Seite „WAGO Device Access“ .....	152
7.1.1.6	Registerkarte „Diagnostic“ .....	153
7.1.1.6.1	Seite „Log Message Viewer“ .....	153
7.1.1.6.2	Seite „Download“ .....	154
7.1.1.6.3	Seite „Network Capture“ .....	154

# 1 Bestimmungen

## 1.1 Gültigkeitsbereich

Das vorliegende Dokument gilt für folgende Produkte:

**750-8110** (PFC100; G2; 2ETH; ECO)

Controller PFC100; 2. Generation; 2 x ETHERNET; ECO

Version Firmware	04.08.xx(30)
Produktdetailseite	<a href="http://www.wago.com/750-8110">http://www.wago.com/750-8110</a>

**750-8111** (PFC100; G2; 2ETH)

Controller PFC100; 2. Generation; 2 x ETHERNET

Version Firmware	04.08.xx(30)
Produktdetailseite	<a href="http://www.wago.com/750-8111">http://www.wago.com/750-8111</a>

**750-8112** (PFC100; G2; 2ETH; RS)

Controller PFC100; 2. Generation; 2 x ETHERNET, RS-232/485

Version Firmware	04.08.xx(30)
Produktdetailseite	<a href="http://www.wago.com/750-8112">http://www.wago.com/750-8112</a>

**750-8112/025-000** (PFC100; G2; 2ETH; RS; T)

Controller PFC100; 2. Generation; 2 x ETHERNET, RS-232/485; Erw. Temperatur

Version Firmware	04.08.xx(30)
Produktdetailseite	<a href="http://www.wago.com/750-8112/025-000">http://www.wago.com/750-8112/025-000</a>

**750-8210** (PFC200; G2; 4ETH)

Controller PFC200; 2. Generation; 4 x ETHERNET

Version Firmware	04.08.xx(30)
Produktdetailseite	<a href="http://www.wago.com/750-8210">http://www.wago.com/750-8210</a>

**750-8210/025-000** (PFC200; G2; 4ETH; T)

Controller PFC200; 2. Generation; 4 x ETHERNET; Erw. Temperatur

Version Firmware	04.08.xx(30)
Produktdetailseite	<a href="http://www.wago.com/750-8210/025-000">http://www.wago.com/750-8210/025-000</a>

**750-8210/040-000** (PFC200; G2; 4ETH; XTR)

Controller PFC200; 2. Generation; 4 x ETHERNET; Extrem

Version Firmware	04.08.xx(30)
Produktdetailseite	<a href="http://www.wago.com/750-8210/040-000">http://www.wago.com/750-8210/040-000</a>

**750-8211** (PFC200; G2; 2ETH 2SFP)

Controller PFC200; 2. Generation; 2 x ETHERNET, 2 x SFP

Version Firmware	04.08.xx(30)
Produktdetailseite	<a href="http://www.wago.com/750-8211">http://www.wago.com/750-8211</a>

**750-8211/040-000** (PFC200; G2; 2ETH 2SFP; XTR)

Controller PFC200; 2. Generation; 2 x ETHERNET, 2 x 100Base-FX; Extrem

Version Firmware	04.08.xx(30)
Produktdetailseite	<a href="http://www.wago.com/750-8211/040-000">http://www.wago.com/750-8211/040-000</a>

**750-8211/040-001** (PFC200; G2; 2ETH 2SFP; Tele; XTR)

Controller PFC200; 2. Generation; 2 x ETHERNET, 2 x 100Base-FX; Fernwirktechnik; Extrem

Version Firmware	04.08.xx(30)
Produktdetailseite	<a href="http://www.wago.com/750-8211/040-001">http://www.wago.com/750-8211/040-001</a>

**750-8212** (PFC200; G2; 2ETH RS)

Controller PFC200; 2. Generation; 2 x ETHERNET, RS-232/-485

Version Firmware	04.08.xx(30)
Produktdetailseite	<a href="http://www.wago.com/750-8212">http://www.wago.com/750-8212</a>

**750-8212/025-000** (PFC200; G2; 2ETH RS; T)

Controller PFC200; 2. Generation; 2 x ETHERNET, RS-232/-485; Erw. Temperatur

Version Firmware	04.08.xx(30)
Produktdetailseite	<a href="http://www.wago.com/750-8212/025-000">http://www.wago.com/750-8212/025-000</a>

**750-8212/025-001** (PFC200; G2; 2ETH RS; Tele; T)

Controller PFC200; 2. Generation; 2 x ETHERNET, RS-232/-485; Fernwirktechnik; Erw. Temperatur

Version Firmware	04.08.xx(30)
Produktdetailseite	<a href="http://www.wago.com/750-8212/025-001">http://www.wago.com/750-8212/025-001</a>

**750-8212/025-002** (PFC200; G2; 2ETH RS; Tele; T; ECO)

Controller PFC200; 2. Generation; 2 x ETHERNET, RS-232/-485; Fernwirktechnik; Erw. Temperatur; ECO

Version Firmware	04.08.xx(30)
Produktdetailseite	<a href="http://www.wago.com/750-8212/025-002">http://www.wago.com/750-8212/025-002</a>

**750-8212/000-100** (PFC200; G2; 2ETH RS BACnet/IP)

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

Version Firmware	04.08.xx(30)
Produktdetailseite	<a href="http://www.wago.com/750-8212/000-100">http://www.wago.com/750-8212/000-100</a>

**750-8212/040-000** (PFC200 G2 2ETH RS XTR)

Controller PFC200 G2; 2 x ETHERNET; RS-232/-485; extrem

Version Firmware	04.08.xx(30)
Produktdetailseite	<a href="http://www.wago.com/750-8212/040-000">http://www.wago.com/750-8212/040-000</a>

**750-8212/040-001** (PFC200 G2 2ETH RS TELE XTR)

Controller PFC200 G2; 2 x ETHERNET; RS-232/-485; Telecontrol; extrem

Version Firmware	04.08.xx(30)
Produktdetailseite	<a href="http://www.wago.com/750-8212/040-001">http://www.wago.com/750-8212/040-001</a>

**750-8212/040-010** (PFC200 G2 2ETH M12 RS XTR)

Controller PFC200 G2; 2 x ETHERNET M12, RS-232/-485; extrem

Version Firmware	04.08.xx(30)
Produktdetailseite	<a href="http://www.wago.com/750-8212/040-010">http://www.wago.com/750-8212/040-010</a>

**750-8213** (PFC200; G2; 2ETH CAN)

Controller PFC200; 2. Generation; 2 x ETHERNET, CAN, CANopen

Version Firmware	04.08.xx(30)
Produktdetailseite	<a href="http://www.wago.com/750-8213">http://www.wago.com/750-8213</a>

**750-8213/040-010** (PFC200 G2 2ETH M12 CAN XTR)

Controller PFC200 G2; 2 x ETHERNET M12, CAN, CANopen; extrem

Version Firmware	04.08.xx(30)
Produktdetailseite	<a href="http://www.wago.com/750-8213/040-010">http://www.wago.com/750-8213/040-010</a>

**750-8214** (PFC200; G2; 2ETH RS CAN)

Controller PFC200; 2. Generation; 2 x ETHERNET, RS-232/-485, CAN, CANopen

Version Firmware	04.08.xx(30)
Produktdetailseite	<a href="http://www.wago.com/750-8214">http://www.wago.com/750-8214</a>

**750-8215** (PFC200; G2; 4ETH CAN USB)

Controller PFC200; 2. Generation; 4 x ETHERNET, CAN, CANopen, USB-A

Version Firmware	04.08.xx(30)
Produktdetailseite	<a href="http://www.wago.com/750-8215">http://www.wago.com/750-8215</a>

**750-8216** (PFC200; G2; 2ETH RS CAN DPS)

Controller PFC200; 2. Generation; 2 x ETHERNET, RS-232/-485, CAN, CANopen, PROFIBUS-Slave

Version Firmware	04.08.xx(30)
Produktdetailseite	<a href="http://www.wago.com/750-8216">http://www.wago.com/750-8216</a>

**750-8216/025-000** (PFC200; G2; 2ETH RS CAN DPS; T)

Controller PFC200; 2. Generation; 2 x ETHERNET, RS-232/-485, CAN, CANopen, PROFIBUS-Slave; Erw. Temperatur

Version Firmware	04.08.xx(30)
Produktdetailseite	<a href="http://www.wago.com/750-8216/025-000">http://www.wago.com/750-8216/025-000</a>

**750-8216/025-001** (PFC200; G2; 2ETH RS CAN DPS; Tele; T)

Controller PFC200; 2. Generation; 2 x ETHERNET, RS-232/-485, CAN, CANopen, PROFIBUS-Slave; Fernwirktechnik; Erw. Temperatur

Version Firmware	04.08.xx(30)
Produktdetailseite	<a href="http://www.wago.com/750-8216/025-001">http://www.wago.com/750-8216/025-001</a>

**750-8216/040-000** (PFC200 G2 2ETH RS CAN DPS XTR)

Controller PFC200 G2; 2 x ETHERNET, RS-232/-485, CAN, CANopen, PROFIBUS-Slave; extrem

Version Firmware	04.08.xx(30)
Produktdetailseite	<a href="http://www.wago.com/750-8216/040-000">http://www.wago.com/750-8216/040-000</a>

**750-8302** (PFC300; 2ETH RS485)

Controller PFC300; 2 x ETHERNET, RS-485

Version Firmware	04.08.xx(30)
Produktdetailseite	<a href="http://www.wago.com/750-8302">http://www.wago.com/750-8302</a>

Die vollständige Gebrauchsanleitung für die Produkte besteht aus mehreren, mitgeltenden Dokumenten. Die Produkte dürfen nur gemäß Anweisungen der vollständigen Gebrauchsanleitung installiert und betrieben werden. Kenntnis aller mitgeltenden Dokumente ist Voraussetzung für die bestimmungsgemäße Verwendung. Alle Dokumente und Informationen finden Sie auf den Produktdetailseiten.

**Mitgeltende Dokumente**

☐ **Systemhandbuch I/O System 750/753**

- Bestimmungen
- Sicherheit
- Planung
- Transport und Lagerung
- Montieren und Demontieren
- Anschließen
- Außer Betrieb nehmen

☐ **Produkthandbuch** des verwendeten Controllers PFC100 G2, PFC200 G2 oder PFC300

- Bestimmungen
- Eigenschaften
- Planung
- Diagnose
- Service

**Information**

Das vorliegende Dokument beschreibt den vollständigen Umfang von Funktionen. Nicht alle beschriebenen Funktionen werden von jedem Produkt unterstützt.

## 2 Überblick

### Controller PFC100

Die Kleinststeuerung PFC100 verfügt über einen 512 MB Speicher und ist damit optimal ausgerüstet für den Einsatz in der Gebäudeindustrie und dem Maschinen- und Anlagenbau.

- Programmierbar mit CODESYS gemäß IEC 61131-1
- Offene Linux®-Plattform
- Umfangreiche Security-Funktionalitäten

### Controller PFC200

Steuerungen der Serie PFC200 verfügen über eine Vielfalt als Funktionen und sind damit gut ausgestattet für den Einsatz in der Industrie-, Prozess- und Gebäudeautomation.

- Feldbusunabhängig
- Programmierbar mit CODESYS gemäß IEC 61131-1 auf einem Linux®-Betriebssystem
- Umfangreiche Security-Funktionalitäten
- XTR-Ausführung für den Einsatz unter extremen Bedingungen

### Controller PFC300

Der PFC300 ist mit 2GB RAM-Speicher und dem 64-Bit-Prozessor optimal ausgestattet für größere Applikationen im Maschinen-, Prozess- und Gebäudeumfeld.

- Programmierbar mit CODESYS gemäß IEC 61131-1 auf einem Linux®-Betriebssystem
- Umfangreiche Security-Funktionalitäten
- Zwei Prozesskerne: DUAL Core
- Serviceschnittstelle USB-C

# 3 Funktionen

## 3.1 Funktionsübersicht

Die hier aufgelisteten Funktionen sind nicht in allen Produkten enthalten.

Die enthaltenen Funktionen finden Sie in der Funktionsübersicht im entsprechenden Produkthandbuch.

Die Funktionen werden in den nachfolgenden Abschnitten beschrieben.

### Systemfunktionen

- [🔗 Produkt- und Systemstatus \[ > 14 \]](#)
- [🔗 Echtzeituhr \[ > 15 \]](#)
- [🔗 Datensicherung \[ > 69 \]](#)
- [🔗 Speicherkartenfunktion \[ > 73 \]](#)
- [🔗 Laufzeitumgebung CODESYS V3 \[ > 16 \]](#)

### Hardwarefunktionen

- [🔗 Betriebsartenschalter/Reset-Taster \[ > 19 \]](#)
- [🔗 Kommunikationsschnittstelle \[ > 21 \]](#)
- [🔗 Service-Schnittstelle \[ > 23 \]](#)
- [🔗 Adresswahlschalter \[ > 19 \]](#)

### Konfigurationsfunktionen

- [🔗 Web-based Management \(WBM\) \[ > 24 \]](#)

### Netzwerkfunktionen

- Netzwerkkonfiguration
- Netzwerksicherheit
- Netzwerkdienste

### Cloud-Connectivity

### Feldbusfunktionen

- [🔗 BACnet \[ > 55 \]](#)
- [🔗 OPC UA \[ > 53 \]](#)
- [🔗 CANopen-Master und -Slave \[ > 59 \]](#)

### Diagnosefunktionen

- [🔗 Diagnose über Anzeigeelemente \[ > 74 \]](#)
- [🔗 Diagnose über WBM \[ > 79 \]](#)

## 3.2 Systemfunktionen

### 3.2.1 Produkt- und Systemstatus

Die Produkteigenschaften werden auf der WBM-Seite „Device Status“ in der Gruppe „Device Details“ angezeigt:

Tabelle 1: WBM-Seite „Device Status“ – Gruppe „Device Details“

Parameter	Bedeutung
Product Description	Bezeichnung des Produktes
Ordernummer	Bestellnummer des Produktes
Unique Item Identifier (UII)	Eindeutige Identifikationsnummer des Produktes
License Information	Anzeige, dass das Laufzeitsystem CODESYS vorhanden ist
Firmware Revision	Firmwarestand

Die wichtigsten Netzwerk- und Schnittstelleneigenschaften des Produktes werden auf der WBM-Seite „Device Status“ in der Gruppe „Network TCP/IP Details“ angezeigt:

Tabelle 2: WBM-Seite „Device Status“ – Gruppe „Network TCP/IP Details“

Parameter	Bedeutung	
DIP Switch Status	Status des Adresswahlschalters; dieser Bereich ist nur sichtbar, wenn ein Adresswahlschalter vorhanden ist.	
DIP Switch Mode	Einstellung des Adresswahlschalters	
	Off (0)	IP-Adressvergabe über z. B. WBM
	static (1 ... 254)	Statische IP-Adressvergabe über Adresswahlschalter
	dhcp (255)	Dynamische IP-Adressvergabe über DHCP
DIP Switch Value	Eingestellter Wert des Adresswahlschalters	
Interface <n>	Aktuell konfiguriertes Interface; Für jedes konfigurierte Interface werden die Eigenschaften in einem separaten Bereich dargestellt.	
Mac Address	MAC-Adresse, die zur Identifikation und Adressierung des Produktes dient	
IP Source	Aktuelle Bezugsart der IP-Adresse	
	none	Es ist keine IP-Vergabemethode ausgewählt; Dies tritt z. B. auf, wenn durch Änderungen an der Bridge-Konfiguration eine Bridge hinzugefügt wurde. Wählen Sie im Register <b>Configuration</b> auf der Seite <b>TCP/IP Configuration</b> eine Bezugsquelle aus.
	static IP	Statische IP-Adressvergabe
	dhcp	Dynamische IP-Adressvergabe über DHCP
	bootp	Dynamische IP-Adressvergabe über BootP
	external	Die IP-Adresse wird ggf. durch die Feldbusapplikation vergeben; Dies tritt z. B. auf, wenn die IP-Adresse durch die Applikation gesteuert wird.
IP Address	Aktuelle IP-Adresse des Produktes	
Subnet Mask	Aktuelle Subnetzmaske des Produktes	

Informationen zum aktivierten Laufzeitsystem werden auf der WBM-Seite „PLC Runtime Information“ in der Gruppe „Runtime“ angezeigt:

Tabelle 3: WBM-Seite „PLC Runtime Information“ – Gruppe „Runtime“

Parameter	Bedeutung
Version	Aktuell aktiviertes Laufzeitsystem Bei ausgeschaltetem Laufzeitsystem wird „None“ angezeigt.

### 3.2.2 Echtzeituhr

#### 3.2.2.1 Anzeige/Manuelle Einstellung

Tabelle 4: WBM-Seite „Clock“ – Gruppe „Timezone and Format“

Parameter	Bedeutung	
Timezone	Zeitzone auswählen, Grundeinstellung:	
	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	„East European Time“, BUL, FI, GR, TR, ...
	CST	„China Standard Time“
JST	„Japan/Korea Standard Time“	
TZ String	Oben nicht auswählbare Zeitzone: Name der Zeitzone, Land und Stadt eingeben Gültigen Namen einer Zeitzone ermitteln: <a href="http://www.timeanddate.com/time/map/">http://www.timeanddate.com/time/map/</a>	
Time Format	Zeitformat: 12h / 24h	
Local Date	Lokales Datum	
Local Time	Lokale Uhrzeit	
UTC Date	Datum	
UTC Time	GMT-Uhrzeit	

#### 3.2.2.2 Automatische Einstellung

Tabelle 5: WBM-Seite „Configuration of NTP Client“ – Gruppe „NTP Client Configuration“

Parameter	Bedeutung
Service enabled	Automatische Aktualisierung der Uhrzeit aktivieren/deaktivieren;
	<input type="checkbox"/> Die Aktualisierung der Uhrzeit ist deaktiviert; Werkseinstellung <input checked="" type="checkbox"/> Die Aktualisierung der Uhrzeit ist aktiviert.
Update Interval (sec)	Aktualisierungsintervall des Time-Servers eingeben.
Time Server <n>	IP-Adressen der Time-Server eingeben; Es sind maximal 4 Time-Server möglich.
Additionally assigned (DHCP)	Durch DHCP zugewiesene NTP-Server; Wenn kein Time-Server zugewiesen wurde, wird „No additional servers assigned“ angezeigt.

### 3.2.3 Laufzeitumgebung CODESYS V3

#### **i Hinweis**

##### **CODESYS V3-Dokumentation lesen!**

Informationen zur Installation, Inbetriebnahme und Programmierung von CODESYS V3 finden Sie im Handbuch zu CODESYS V3.

#### **i Hinweis**

##### **Nicht benötigte Ports und Dienste schließen!**

Durch geöffnete Ports können Unbefugte Zugriff auf Ihr Automatisierungssystem erhalten.

1. Um die Gefahr von Cyberangriffen zu verringern und damit die Cyber-Security zu erhöhen, schließen Sie alle nicht von Ihrer Applikation benötigten Ports und Dienste in den Steuerungskomponenten (z. B. Port 6626 für WAGO-I/O-CHECK und Port 11740 für CODESYS V3).
2. Öffnen Sie die Ports und Dienste nur für die Dauer der Inbetriebnahme bzw. Konfiguration.

#### **i Hinweis**

##### **CODESYS Dienste werden bei eingeschalteter Firewall ohne User-Filter abgewiesen!**

Wenn CODESYS Dienste (z. B. Modbus, OPC-UA, SNMP oder IIOT) genutzt werden, müssen in der Firewall-Konfiguration User-Filter für diese Dienste angelegt werden. Die User-Filter müssen so konfiguriert sein, dass die entsprechenden Ports akzeptiert werden.

#### 3.2.3.1 Speicherbereiche unter CODESYS V3

##### 3.2.3.1.1 Programm- und Datenspeicher

Der Programm- (auch Code-) und Datenspeicher ist nach dem erfolgreichen Programm-Download im System bereits angefordert worden und kann vollständig genutzt werden. Der Speicherbereich wird zwischen Programm und Daten dynamisch aufgeteilt. Die Gesamtgröße ist produktabhängig und in den technischen Daten zum jeweiligen Produkt angegeben.

##### 3.2.3.1.2 Bausteinbegrenzung

Zusammen mit dem von der Applikation nutzbaren Programm- und Datenspeicher wird für die einzelnen Programmteile im System Speicher zur Verwaltung benötigt. Die Größe dieses Verwaltungsbereiches berechnet sich aus Bausteinbegrenzung  $\times$  12. Die Summe aus globalen Programm- und Datenspeicher und Bausteinbegrenzungsspeicher ergibt die tatsächliche Größe des im System für Daten angeforderten Arbeitsspeichers.

##### 3.2.3.1.3 Merkerbereich (Memory) und Retain-Bereich

Der Merkerbereich (Memory) und der Retain-Bereich bilden zusammen den remanenten Speicher für die IEC-61131-Anwendung. Die Gesamtgröße ist produktabhängig und in den technischen Daten zum jeweiligen Produkt angegeben.

### 3.2.3.2 CODESYS V3-Prioritäten

In Ergänzung zur CODESYS V3-Dokumentation finden Sie hier eine Auflistung der für den Controller implementierten Prioritäten.

Tabelle 6: CODESYS V3-Prioritäten

Scheduler	Aufgabe	Linux®-Priorität	IEC-Priorität	Bemerkung
Preemptives Scheduling - Echtzeitbereich	Lokal- oder Feldbus - HIGH	-95 ... -86		Lokalbus (-88)
	Betriebsartenschalter Überwachung	-85		Task registriert Änderungen des Betriebsartenschalters und ändert den Zustand der SPS-Applikation. (Start, Stop, Reset Warm/Kalt)
	CODESYS Watchdog	-83		Ausführung der Watchdog- Funktionalitäten
	Zyklische und ereignisgesteuerte IEC-Task	-55 ... -53	1 ... 3	Für Echtzeitaufgaben, deren Ausführung nicht von externen Schnittstellen (z. B.: Feldbus) beeinflusst werden darf.
	Lokal- oder Feldbus - MID	-52 ... -43		CAN (-52 ... -51) PROFIBUS (-49 ... -45) Modbus-Slave/ Master (-43)
	Zyklische und ereignisgesteuerte IEC-Task	-42 ... -32	4 ... 14	Für Echtzeitaufgaben, deren Ausführung die Feldbuskommunikation nicht beeinflussen darf.
	Lokal- oder Feldbus - LOW	-13 ... -4		
Fair Scheduling - Nicht-Echtzeitbereich	CODESYS Kommunikation	Background (20)		Kommunikation mit der CODESYS Entwicklungsumgebung
	Zyklische, ereignisgesteuerte und freilaufende IEC-Task		15	u. a. Standardpriorität der Visualisierungstask

### 3.2.3.3 CODESYS V3-Dienst- und Porteinstellungen

Tabelle 7: WBM-Seite „PLC Runtime Configuration“ – Gruppe „General PLC Runtime Configuration“

Parameter	Bedeutung	
PLC Runtime Version	Auswahl des aktiven SPS-Laufzeitsystems	
	none	Es ist kein Laufzeitsystem aktiviert.
	CODESYS V3	Das Laufzeitsystem CODESYS V3 ist aktiviert.
Home directory on memory card enabled	Auswahl des Speicherortes für das Home-Verzeichnis des Laufzeitsystems	
	<input type="checkbox"/>	Das Home-Verzeichnis wird im internen Speicher abgelegt.
	<input checked="" type="checkbox"/>	Das Home-Verzeichnis wird auf die Speicherkarte ausgelagert.

Tabelle 8: WBM-Seite „PLC Runtime Configuration“ – Gruppe „Webserver Configuration“

Parameter	Bedeutung	
CODESYS 3 Webserver State	Status (enabled/disabled) des CODESYS V3-Webservers	
Default Webserver	Auswahl der Seitenanzeige bei alleiniger Eingabe der IP-Adresse des Produktes	
	Web-Based- Management	Das Web-Based-Management wird angezeigt.
	WebVisu	Die Webvisualisierung des Laufzeitsystems wird angezeigt.

Tabelle 9: WBM-Seite „PLC Runtime Services“ – Gruppe „CODESYS V3“

Parameter	Bedeutung	
CODESYS V3 State	Status des Laufzeitsystems	
	disabled	Das Laufzeitsystem ist deaktiviert.
	enabled	Das Laufzeitsystem ist aktiviert.
Webserver Enabled	Webserver für die Webvisualisierung aktivieren/deaktivieren.	
	<input type="checkbox"/>	Der Webserver ist deaktiviert.
	<input checked="" type="checkbox"/>	Der Webserver ist aktiviert.
Separated WebVisu Ports (8080/8081)	CODESYS WebVisu-Ports für HTTP/HTTPS einstellen.	
	<input type="checkbox"/>	Die CODESYS WebVisu wird auf den Ports 80/443 bereitgestellt (Standard wie WBM).
	<input checked="" type="checkbox"/>	Die CODESYS WebVisu wird auf den Ports 8080/8081 bereitgestellt.
Port Authentication Enabled	Log-in für die Verbindung zum Gerät aktivieren/deaktivieren.	
	<input type="checkbox"/>	Für die Verbindung ist kein Log-in erforderlich.
	<input checked="" type="checkbox"/>	Für die Verbindung ist ein Log-in erforderlich. Der Standard-Benutzername ist admin und das Passwort ist das unter „General Configuration“ angegebene Passwort.
Webserver Port Authentication Enabled	Log-in für den Aufruf der Webvisualisierung einer Codesys-Applikation aktivieren/deaktivieren.	
	<input type="checkbox"/>	Für den Aufruf der Webvisualisierung ist kein Log-in erforderlich.
	<input checked="" type="checkbox"/>	Für den Aufruf der Webvisualisierung ist ein Log-in erforderlich. Der Standard-Benutzername ist admin und das Passwort ist das unter „General Configuration“ angegebene Passwort.

### 3.3 Hardwarefunktionen

#### 3.3.1 Adresswahlschalter

#### 3.3.2 Betriebsartenschalter/Reset-Taster

##### 3.3.2.1 Betriebsartenschalter/Reset-Taster aktivieren/deaktivieren

Vor allem aus Sicherheitsgründen und für schwer zugängliche Installationen bietet der Controller die Möglichkeit, den Betriebsartenschalter und den Reset-Taster zu aktivieren bzw. zu deaktivieren.

Bei deaktiviertem Betriebsartenschalter muss die Steuerung über die CODESYS Entwicklungsumgebung kontrolliert werden.

Bei deaktiviertem Reset-Taster ist ein Software-Reset (Neustart) weiterhin über das WBM möglich.

#### Hinweis

**Bei deaktiviertem Betriebsartenschalter wird ein geladenes CODESYS Boot-Projekt automatisch nach dem Neustart des Produktes ausgeführt!**

Das Stoppen und Zurücksetzen einer laufenden Applikation ist bei deaktiviertem Betriebsartenschalter nur über die CODESYS Entwicklungsumgebung möglich.

Die Einstellung erfolgt auf der WBM-Seite „Controls Settings“ im Register „Configuration“. Eine Änderung wird erst nach einem Neustart des Controllers wirksam.

Tabelle 10: WBM-Seite „Controls Settings“ – Gruppe „OMS Controls“

Parameter	Bedeutung	
Current Mode	Aktueller Status der Funktionalität des Betriebsartenschalters und des Reset-Tasters	
	Inactive	Der Controller ignoriert jede Betätigung des Betriebsartenschalters und des Reset-Tasters.
	Active	Controller reagiert auf eine Betätigung des Betriebsartenschalters und des Reset-Tasters.
Activate	Aktivierung/Deaktivierung des Betriebsartenschalters und des Reset-Tasters	
	<input type="checkbox"/>	Betriebsartenschalter und Reset-Taster deaktivieren.
	<input checked="" type="checkbox"/>	Betriebsartenschalter und Reset-Taster aktivieren.

##### 3.3.2.2 Temporär feste IP-Adressen einstellen

Mit diesem Vorgang werden die IP-Adressen für die Netzwerkschnittstellen X1 ... X<n> temporär auf feste IP-Adressen eingestellt.

Für jede verwendete Bridge wird dabei den zugeordneten Schnittstellen eine eigene Adresse vergeben, wobei Bridge 1 die IP-Adresse „192.168.1.17“, Bridge 2 die IP-Adresse „192.168.2.17“ usw. erhält.

Es wird kein Reset durchgeführt.

Um temporär feste IP-Adressen einzustellen, gehen Sie folgendermaßen vor:

1. Bringen Sie den Betriebsartenschalter in die STOP-Position.

2. Betätigen Sie den Reset-Taster länger als 8 Sekunden.

➔ Die Ausführung wird durch eine orange blinkende „SYS“-LEDs signalisiert.

Wenn Sie nach dem Aktivieren der temporären IP-Adressen Änderungen an der IP-Konfiguration einer Bridge vornehmen, werden die neuen Einstellungen permanent übernommen und sofort angewendet. Die konfigurierte Bridge verlässt somit den temporären IP-Adressmodus. Die anderen Bridges behalten bis zum Neustart/Reset die temporär eingestellte IP-Adresse.

Um die Einstellung wieder aufzuheben, gehen Sie folgendermaßen vor:

- Führen Sie einen Software-Reset durch,
- oder
- Schalten sie das Produkt aus und wieder ein.

### 3.3.2.3 Software-Reset (Neustart)

- Um einen Software-Reset durchzuführen, bringen Sie den Betriebsartenschalter in die „RUN“- oder „STOP“-Position und betätigen Sie den Reset-Taster länger als 1 Sekunde aber kürzer als 8 Sekunden.
- ➔ Die Ausführung wird durch ein kurzes Aufleuchten aller LEDs signalisiert. Nach einigen weiteren Sekunden signalisiert die „SYS“-LED den erfolgreichen Bootvorgang des Controllers.

### 3.3.2.4 Controller-Reset

#### **ACHTUNG**

##### **Controller nicht ausschalten!**

Durch eine Unterbrechung des Reset-Vorgangs kann der Controller beschädigt werden.

- Schalten Sie den Controller während des Reset-Vorgangs nicht aus und unterbrechen Sie nicht die Spannungsversorgung!

Bei einem Zurücksetzen des Controllers („Controller-Reset“) werden:

- Parameter und Passwörter der Linux- und WBM-Benutzer des Controllers überschrieben,
- gespeicherte Boot-Projekte einschließlich vorhandener Webvisualisierungen gelöscht,
- nachinstallierte Firmwarefunktionen nicht überschrieben,
- Software-Lizenzen nicht gelöscht,

Das inaktive System wird durch den Controller-Reset nicht verändert.

Bei Rückfragen wenden Sie sich an den WAGO Support.

Nach dem Controller-Reset wird der Controller automatisch neu gestartet.

Um einen Controller-Reset durchzuführen, gehen Sie wie folgt vor:

✓ Voraussetzung: Spannungsversorgung ist aktiv.

1. Betätigen Sie den Reset-Taster und halten Sie ihn gedrückt.
2. Schieben Sie den Betriebsartenschalter in die Position „RESET“ und halten Sie ihn in dieser Position.
3. Halten Sie beide Taster bis die „SYS“-LED im Wechsel rot/grün blinkt (ca. 8 Sekunden).

4. Lassen Sie den Betriebsartenschalter und den Reset-Taster los.
- ➔ Der Controller wurde zurückgesetzt und führt einen automatischen Neustart aus.

### 3.3.3 Kommunikationsschnittstelle

#### 3.3.3.1 PFC100/PFC200

Der Controller verfügt über eine konfigurierbare Kommunikationsschnittstelle.

Die Betriebsart der Schnittstelle ist zwischen RS-232 und RS-485 umschaltbar.

Die Schnittstelle unterstützt folgende Kommunikationsparameter:

- 8 Datenbits
- Gerade/ungerade Parität
- 0/1/2 Stopbits

Die Kommunikationsschnittstelle kann der Linuxkonsole zugewiesen werden. In diesen Fall kann nur die Linuxkonsole über die Schnittstelle kommunizieren.

Wenn die Schnittstelle nicht zugeordnet ist, kann beispielsweise das CODESYS Programm über Funktionsbausteine darauf zugreifen.

Die Einstellung der Kommunikationsschnittstelle erfolgt z. B. über die WBM-Seite „Configuration of Serial Interface“.

Die aktuelle Konfiguration der Schnittstelle wird in der Gruppe „Current Serial Interface Configuration“ angezeigt.

Tabelle 11: WBM-Seite „Configuration of Serial Interface“ – Gruppe „Current Serial Interface Configuration“

Parameter	Bedeutung	
Assigned to	Zuordnung der Kommunikationsschnittstelle	
	Unassigned (usage by Applications, Libraries, PLC Runtime)	Die Kommunikationsschnittstelle ist keiner Applikation zugewiesen. Damit kann beispielsweise das CODESYS Programm über Funktionsbausteine darauf zugreifen.
	Linux Console	Die Kommunikationsschnittstelle ist der Linuxkonsole zugewiesen.
Mode	Modus der Kommunikationsschnittstelle	
	RS232	Die Kommunikationsschnittstelle wird im RS-232-Modus betrieben.
	RS485	Die Kommunikationsschnittstelle wird im RS-485-Modus betrieben.

Die Zuordnung der Schnittstelle wird in der Gruppe „Assign Owner of Serial Interface“ eingestellt.

Tabelle 12: WBM-Seite „Configuration of Serial Interface“ – Gruppe „Assign Owner of Serial Interface“

Parameter	Bedeutung
Unassigned (usage by Applications, Libraries, PLC Runtime)	Die Kommunikationsschnittstelle wird keiner Applikation zugewiesen.
Linux Console	Die Kommunikationsschnittstelle wird der Linuxkonsole zugewiesen.

Die Betriebsart der Schnittstelle wird in der Gruppe „Assign Mode of Serial Interface“ eingestellt.

Tabelle 13: WBM-Seite „Configuration of Serial Interface“ – Gruppe „Assign Mode of Serial Interface“

Parameter	Bedeutung
RS232	Die Kommunikationsschnittstelle wird im RS-232-Modus betrieben.
RS485	Die Kommunikationsschnittstelle wird im RS-485-Modus betrieben.

### 3.3.3.2 PFC300

Der Controller verfügt über eine konfigurierbare Kommunikationsschnittstelle.

Die Betriebsart der Schnittstelle ist fest auf RS-485 eingestellt.

Die Schnittstelle unterstützt folgende Kommunikationsparameter:

- 8 Datenbits
- Gerade/ungerade Parität
- 0/1/2 Stoppbits

Ein Biasing-Netzwerk verhindert Schwingungen auf den Busleitungen, wenn kein Sender aktiv ist. Diese Schwingungen können zu Übertragungsfehlern führen. Pull-up- und Pull-down-Widerstände gewährleisten, dass im Ruhezustand alle Empfängereingänge eine Spannungsdifferenz zwischen RxD+ und RxD- von mehr als 200 mV aufweisen.

Ein Abschlusswiderstand an jedem Ende der Busleitungen verhindert Reflexionen auf den Busleitungen. Diese Reflexionen können ebenfalls zu Übertragungsfehlern führen.

Entsprechend den Anforderungen an den Bus können die in der Schnittstelle integrierten Pull-up- und Pull-down-Widerstände (1) des Bias-Netzwerkes und der integrierte Abschlusswiderstand (2) ein- oder ausgeschaltet werden.

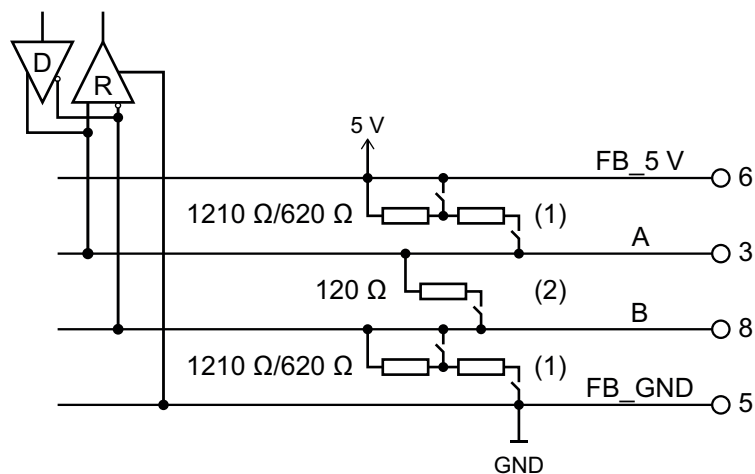


Abbildung 1: Kommunikationsschnittstelle, Busabschluss und Bias-Netzwerk

Die Einstellung der Kommunikationsschnittstelle erfolgt z. B. über die WBM-Seite „Configuration of Serial Interface“.

Die aktuelle Konfiguration der Schnittstelle wird in der Gruppe „Current Serial Interface Configuration“ angezeigt.

Tabelle 14: WBM-Seite „Configuration of Serial Interface“ – Gruppe „Current Serial Interface Configuration“

Parameter	Bedeutung
Mode	Modus der Kommunikationsschnittstelle
	RS485 Die Kommunikationsschnittstelle wird im RS-485-Modus betrieben.

Der Busabschluss ist in der Gruppe „Bus Termination“ einstellbar.

Tabelle 15: WBM-Seite „Configuration of Serial Interface“ – Gruppe „Bus Termination“

Parameter	Bedeutung	
Termination enabled	Busabschluss aktivieren/deaktivieren.	
	<input type="checkbox"/>	Der Busabschluss ist deaktiviert.
	<input checked="" type="checkbox"/>	Der Busabschluss ist aktiviert.

Das Bias-Netzwerk ist in der Gruppe „Bias Network“ einstellbar.

Tabelle 16: WBM-Seite „Configuration of Serial Interface“ – Gruppe „Bias Network“

Parameter	Bedeutung
Off	Kein Bias-Netzwerk ist aktiv.
Low	Das Bias-Netzwerk 1 (640 Ohm) ist aktiv.
High	Das Bias-Netzwerk 2 (1210 Ohm) ist aktiv.

### 3.3.4 Service-Schnittstelle

Die Einstellung der Service-Schnittstelle erfolgt z. B. über die WBM-Seite „Configuration of Service Interface“.

Zuordnung der Schnittstelle:

Tabelle 17: WBM-Seite „Configuration of Service Interface“ – Gruppe „Assign Owner of Service Interface“

Parameter	Bedeutung
WAGO Service Communication	Die Service-Schnittstelle wird für die WAGO Service-Kommunikation bzw. Laufzeitsystem-Kommunikation verwendet.
Linux Console	Die Service-Schnittstelle ist der Linux-Konsole zugewiesen.
Unassigned (usage by Applications, Libraries, PLC Runtime)	Die Service-Schnittstelle ist keiner Applikation zugewiesen. Damit kann beispielsweise das CODESYS Programm über Funktionsbausteine darauf zugreifen.

### 3.4 Konfigurationsfunktionen

#### 3.4.1 Web-based Management (WBM)

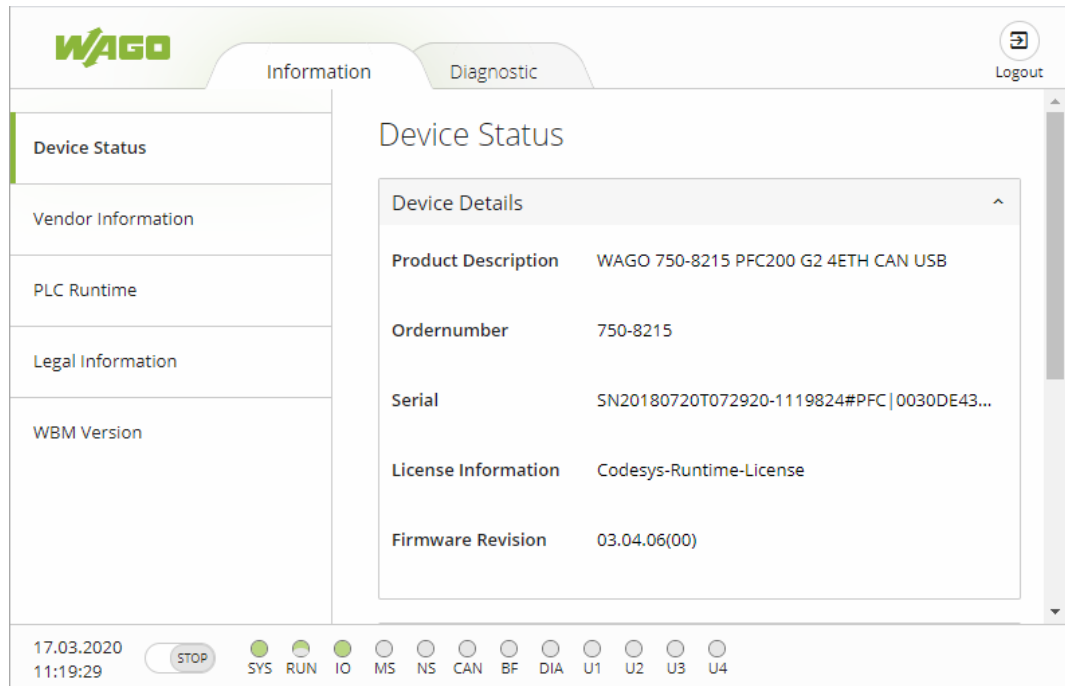


Abbildung 2: WBM-Browserfenster (Beispiel)

In der Kopfzeile des Browserfensters werden die Registerkarten für die verschiedenen WBM-Bereiche sowie die Schaltflächen **[Reboot]** und **[Logout]** angezeigt. Die Schaltfläche **[Reboot]** ist nur sichtbar, wenn Sie als Administrator angemeldet sind. Über die Schaltfläche **[Reboot]** können Sie einen Neustart des Controllers ausführen. Ein Neustart kann einige Minuten dauern. Über die Schaltfläche **[Logout]** melden Sie den aktuellen Benutzer ab, wenn Sie die Oberfläche nicht weiter verwenden möchten. Sie gelangen dann wieder zur Anmeldeaufforderung.

Wenn nicht alle Registerkarten in der gewählten Breite des Fensters darstellbar sind, wird anstelle der nicht darstellbaren Registerkarten eine Registerkarte mit Auslassungszeichen (...) angezeigt. Damit können Sie über ein Pull-down-Menü die nicht dargestellten Registerkarten auswählen.

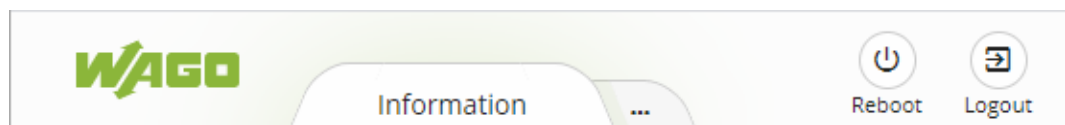


Abbildung 3: WBM-Kopfzeile mit nicht darstellbaren Registerkarten (Beispiel)

Auf der linken Seite des Browserfensters wird der Navigationsbaum angezeigt. Der Inhalt des Navigationsbaums ist abhängig von der ausgewählten Registerkarte. Über den Navigationsbaum können Sie die einzelnen Seiten und, falls vorhanden, deren Unterseiten erreichen.

In der Statuszeile wird der aktuelle Gerätezustand angezeigt.

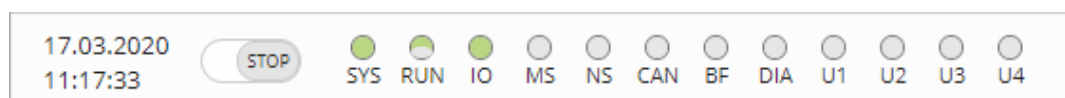


Abbildung 4: WBM-Statuszeile (Beispiel)

- Datum und Uhrzeit – lokale Zeit und lokales Datum auf dem Gerät
- Zustand des Betriebsartenschalters
- LED-Zustände des Gerätes:  
Die LEDs sind mit ihrer jeweiligen Bezeichnung (z. B. SYS, RUN, IO, ...) beschriftet und die Zustände werden über eine Grafik symbolisiert. Es sind folgende Darstellungen möglich:
  - Grau: Die LED ist ausgeschaltet.
  - Vollflächige Farbe: Die LED ist in der jeweiligen Farbe eingeschaltet.
  - Halbflächige Farbe: Die LED blinkt in der entsprechenden Farbe. Die andere Hälfte der Fläche ist dann entweder grau oder ebenfalls gefärbt. Letzteres bedeutet, dass die LED sequenziell in verschiedenen Farben blinkt.
 Solange der Mauszeiger sich über einer LED befindet, öffnet sich ein Tooltip mit weiteren Informationen. Der angezeigte Text enthält die Meldung, die die LED in ihren aktuellen Zustand versetzt hat. Hier ist auch die Zeitangabe der Meldung enthalten.  
Die im WBM angezeigten Zustände entsprechen nicht zu jedem Zeitpunkt genau denen auf dem Controller. Die Daten haben bei der Übertragung eine Laufzeit und können auch nur in einem bestimmten Intervall abgefragt werden. Die Zeitdauer zwischen zwei Abfragen beträgt 30 Sekunden.

## 3.5 Netzwerkfunktionen

### 3.5.1 Netzwerkkonfiguration

#### 3.5.1.1 Schnittstellenkonfiguration

##### 3.5.1.1.1 Bridge-Konfiguration

Tabelle 18: WBM-Seite „Ethernet Configuration“ – Gruppe „Bridge Configuration“

Parameter	Bedeutung
Bridge 1 ... <n>	Zuordnung der physikalischen Ports X1 ... X<n> zu einer logischen Bridge; Klicken Sie dazu die entsprechende Optionsschaltfläche. Die Zuordnung wird farblich markiert. Ein Port kann immer nur einer Bridge zugeordnet werden.

##### 3.5.1.1.2 Dummy-Interfaces

Tabelle 19: WBM-Seite „Ethernet Configuration“ – Gruppe „Dummy Interfaces“

Parameter	Bedeutung
Name	Name des ausgewählten Dummy-Interfaces

##### 3.5.1.1.3 VLAN-Interfaces

Tabelle 20: WBM-Seite „Ethernet Configuration“ – Gruppe „VLAN Interfaces“

Parameter	Bedeutung
Name	Name des ausgewählten VLAN-Interfaces
VLAN-ID	VLAN-ID des ausgewählten VLAN-Interfaces
Link	Zugeordnete Bridge des ausgewählten VLAN-Interfaces

##### 3.5.1.1.4 Port Mirror-Konfiguration (PFC100 G2, PFC200 G2 - 2-Port, PFC300)

Tabelle 21: WBM-Seite „Ethernet Configuration“ – Gruppe „Port Mirror Settings“

Parameter	Bedeutung
Enabled	Spiegelung des Datenverkehrs zwischen den Ports ein-/ausschalten.

Parameter	Bedeutung	
	<input type="checkbox"/>	Datenverkehr wird nicht gespiegelt (Werkseinstellung).
	<input checked="" type="checkbox"/>	Datenverkehr wird zwischen den ausgewählten Ports gespiegelt.
Source	Quellport des gespiegelten Datenverkehrs (X1 ... X<n>)	
Destination	Zielpport des gespiegelten Datenverkehrs (X1 ... X<n>)	

### 3.5.1.1.5 Storm Control-Konfiguration (PFC100 G2, PFC200 G2 - 2-Port)

Tabelle 22: WBM-Seite „Ethernet Configuration“ – Gruppe „Storm Control Settings“

Parameter	Bedeutung	
Broadcast Protection	Grenzwert der Datenpakete für Broadcast; Defaultwert: 1 % der maximalen Datenrate	
Multicast Protection	Einstellung, ob die Begrenzung der Datenpakete nur für Broadcast oder für Broadcast und Multicast gemeinsam gilt	
	<input type="checkbox"/>	Begrenzung der Datenpakete gilt nur für Broadcast-Pakete.
	<input checked="" type="checkbox"/>	Begrenzung der Datenpakete gilt für Broadcast- und Multicast-Pakete gemeinsam.

### 3.5.1.1.6 Storm Control-Konfiguration (PFC200 G2 - 4-Port)

Tabelle 23: WBM-Seite „Ethernet Configuration“ – Gruppe „Storm Control Settings“

Parameter	Bedeutung	
Broadcast Protection	Grenzwert der Datenpakete für Broadcast; Defaultwert: 1 Mbits	
Multicast Protection	Grenzwert der Datenpakete für Multicast; Defaultwert: 1 Mbits	

### 3.5.1.1.7 Storm Control-Konfiguration (PFC300)

Tabelle 24: WBM-Seite „Ethernet Configuration“ – Gruppe „Storm Control Settings“

Parameter	Bedeutung	
Broadcast Protection	Grenzwert der Datenpakete für Broadcast; Defaultwert: 20000 Pakete pro Sekunde	
Multicast Protection	Grenzwert der Datenpakete für Multicast; Defaultwert: 20000 Pakete pro Sekunde	

### 3.5.1.1.8 Ethernet Interface-Konfiguration (PFC100 G2, PFC200 G2 - 2-Port)

Tabelle 25: WBM-Seite „Ethernet Configuration“ – Gruppen „Ethernet Interface Configuration“

Parameter	Bedeutung	
Interface X<n>	Für jedes im Controller vorhandenes Interface wird ein eigener Bereich angezeigt.	
Enabled	Interface aktivieren/deaktivieren.	
	<input type="checkbox"/>	Das Interface ist deaktiviert.
	<input checked="" type="checkbox"/>	Das Interface ist aktiviert.
MAC Learning	„MAC Learning“-Funktionalität für das Interface aktivieren/deaktivieren.	
	<input type="checkbox"/>	Die „MAC Learning“-Funktionalität ist deaktiviert.
	<input checked="" type="checkbox"/>	Die „MAC Learning“-Funktionalität ist aktiviert.

Parameter	Bedeutung
Broadcast Protection Enabled	Broadcast-Protection aktivieren/deaktivieren.
	<input type="checkbox"/> Broadcast-Protection ist deaktiviert.
	<input checked="" type="checkbox"/> Broadcast-Protection ist aktiviert.
Current Speed/Duplex	Aktuelle Übertragungsgeschwindigkeit und aktuelles Übertragungsverfahren
Speed/Duplex	Übertragungsgeschwindigkeit und Übertragungsverfahren auswählen; Die Auswahlliste wird geräte- und interfaceabhängig generiert. Mit der Auswahl „Autonegotiation“ werden die Verbindungsmodalitäten automatisch mit der Gegenstelle ausgehandelt.

### 3.5.1.1.9 Ethernet Interface-Konfiguration (PFC200 G2 - 4-Port, PFC300)

Tabelle 26: WBM-Seite „Ethernet Configuration“ – Gruppen „Ethernet Interface Configuration“

Parameter	Bedeutung
Interface X<n>	Für jedes im Controller vorhandenes Interface wird ein eigener Bereich angezeigt.
Enabled	Interface aktivieren/deaktivieren.
	<input type="checkbox"/> Das Interface ist deaktiviert.
	<input checked="" type="checkbox"/> Das Interface ist aktiviert.
MAC Learning	„MAC Learning“-Funktionalität für das Interface aktivieren/deaktivieren.
	<input type="checkbox"/> Die „MAC Learning“-Funktionalität ist deaktiviert.
	<input checked="" type="checkbox"/> Die „MAC Learning“-Funktionalität ist aktiviert.
Broadcast Protection Enabled	Broadcast-Protection aktivieren/deaktivieren.
	<input type="checkbox"/> Broadcast-Protection ist deaktiviert.
	<input checked="" type="checkbox"/> Broadcast-Protection ist aktiviert.
Multicast Protection Enabled	Multicast-Protection aktivieren/deaktivieren.
	<input type="checkbox"/> Multicast-Protection ist deaktiviert.
	<input checked="" type="checkbox"/> Multicast-Protection ist aktiviert.
Current Speed/Duplex	Aktuelle Übertragungsgeschwindigkeit und aktuelles Übertragungsverfahren
Speed/Duplex	Übertragungsgeschwindigkeit und Übertragungsverfahren auswählen; Die Auswahlliste wird geräte- und interfaceabhängig generiert. Mit der Auswahl „Autonegotiation“ werden die Verbindungsmodalitäten automatisch mit der Gegenstelle ausgehandelt.

### 3.5.1.2 TCP/IP-Konfiguration

#### 3.5.1.2.1 Bridge-Interfaces

Tabelle 27: WBM-Seite „TCP/IP Configuration“ – Gruppe „Bridge Interfaces“

Parameter	Bedeutung
Bridge <n>	Einstellungen für die ausgewählte Bridge
Current IP Address	Aktuelle IP-Adresse
Current Subnet Mask	Aktuelle Subnetzmaske
Current Default Gateway	IP-Adresse des aktuellen Default-Gateways
IP Source	IP-Adressierung auswählen.

Parameter	Bedeutung	
	Static IP	Statische IP-Adressierung
	DHCP	Dynamische IP-Adressierung über DHCP
	BootP	Dynamische IP-Adressierung über BootP
Static IP Address	Statische IP-Adresse eingeben; die IP-Adresse ist aktiv, wenn im Auswahlfeld <b>IP Source</b> „Static IP“ aktiviert ist.	
Subnet Mask	Subnetzmaske eingeben; die Subnetzmaske ist aktiv, wenn im Auswahlfeld <b>IP Source</b> „Static IP“ aktiviert ist.	
Default Gateway	IP-Adresse des Default-Gateways eingeben	

### 3.5.1.2.2 Dummy-Interfaces

Tabelle 28: WBM-Seite „TCP/IP Configuration“ – Gruppe „Dummy Interfaces“

Parameter	Bedeutung	
Dummy <n>	Einstellungen für das ausgewählte Dummy-Interface	
Current IP Address	Aktuelle IP-Adresse	
Current Subnet Mask	Aktuelle Subnetzmaske	
IP Source	IP-Adressierung auswählen.	
	Static IP	Statische IP-Adressierung
Static IP Address	Statische IP-Adresse eingeben; die IP-Adresse ist aktiv, wenn im Auswahlfeld <b>IP Source</b> „Static IP“ aktiviert ist.	
Subnet Mask	Subnetzmaske eingeben; die Subnetzmaske ist aktiv, wenn im Auswahlfeld <b>IP Source</b> „Static IP“ aktiviert ist.	

### 3.5.1.2.3 VLAN-Interfaces

Tabelle 29: WBM-Seite „TCP/IP Configuration“ – Gruppe „VLAN Interfaces“

Parameter	Bedeutung	
VLAN <n>	Einstellungen für das ausgewählte VLAN-Interface	
Current IP Address	Aktuelle IP-Adresse	
Current Subnet Mask	Aktuelle Subnetzmaske	
IP Source	IP-Adressierung auswählen.	
	Static IP	Statische IP-Adressierung
	DHCP	Dynamische IP-Adressierung
Static IP Address	Statische IP-Adresse eingeben; die IP-Adresse ist aktiv, wenn im Auswahlfeld <b>IP Source</b> „Static IP“ aktiviert ist.	
Subnet Mask	Subnetzmaske eingeben; die Subnetzmaske ist aktiv, wenn im Auswahlfeld <b>IP Source</b> „Static IP“ aktiviert ist.	

### 3.5.1.2.4 DNS-Server

Der Controller kann maximal 3 aktive DNS-Server nutzen.  
DNS-Server können über DHCP oder manuell zugewiesen werden.

Die tatsächlich verwendeten DNS-Server ergeben sich durch eine abwechselnde Zusammenführung der über DHCP zugewiesenen DNS-Server und der manuell zugewiesenen DNS-Server.

Der erste DNS-Server, der über DHCP zugewiesen wurde, erhält die höchste Priorität.

Die Anzeige der zugewiesenen DNS-Server und die manuelle Zuweisung weiterer DNS-Server ist z. B. über die WBM-Seite „TCP/IP Configuration“ in der Gruppe „DNS Server“ möglich.

Tabelle 30: WBM-Seite „TCP/IP Configuration“ – Gruppe „DNS Server“

Parameter	Bedeutung
Active	Aktive DNS-Server; Der Index spiegelt die Anfrage-Reihenfolge wider.
Assigned by DHCP	Durch DHCP (oder BootP) zugewiesene DNS-Server; Wenn kein DNS-Server durch DHCP (oder BootP) zugewiesen wurde, wird „no DNS Servers assigned by DHCP“ angezeigt.
Assigned by user	Adressen der vom Benutzer eingetragenen DNS-Server; Wenn kein Server eingetragen wurde, erscheint die Anzeige „no DNS Servers configured“.

### 3.5.1.3 Hostname/Domainname

#### 3.5.1.3.1 Hostname

Ohne eine Konfiguration eines Hostnamens bekommt der Controller einen Standardnamen, in den die letzten drei Werte der MAC-Adresse des Controllers eingehen. Dieser Name gilt, solange noch kein Hostname konfiguriert wurde bzw. kein Hostname per DHCP an den Controller geliefert wurde (zur Konfiguration des Controllers siehe Kapitel „In Betrieb nehmen“ > „Konfigurieren“). Bei der Einstellung des Hostnamens ist zu beachten, dass ein per DHCP-Antwort gelieferter Hostname sofort aktiv wird und den konfigurierten bzw. Standardhostnamen verdrängt.

Bei mehreren Netzwerkschnittstellen mit DHCP wird der Hostname von der Netzwerkschnittstelle (Bridge oder Wwan) mit der höchsten Priorität übernommen. Die Priorität ist alphanumerisch durch den Namen der Netzwerkschnittstelle festgelegt. Somit hat die Bridge1 die höchste Priorität gefolgt von Bridge2, Bridge3, ..., Wwan0.

Falls nur der konfigurierte Name gelten soll, muss der Netzwerkadministrator die Konfiguration des aktiven DHCP-Servers so anpassen, dass keine Hostnamen in der DHCP-Antwort übertragen werden.

Der Standardhostname bzw. der konfigurierte Name wird wieder aktiv, wenn die Netzwerkschnittstellen auf statische IP-Adressen umgestellt werden oder noch kein Hostname per DHCP-Antwort eingetroffen ist.

Die Einstellungen zum Hostnamen sind z. B. auf der WBM-Seite „Configuration of Host- and Domain Name“ in der Gruppe „Host Name“ möglich.

Tabelle 31: WBM-Seite „Configuration of Host- and Domain Name“ – Gruppe „Hostname“

Parameter	Bedeutung
Currently used	Aktuell verwendeter Hostname
Configured	Optionalen Hostnamen eingeben
[Clear]	Optionalen Hostnamen löschen und Standardwert wiederherstellen

#### 3.5.1.3.2 Domainname

Für einen Domainnamen gilt ein ähnlicher Mechanismus wie für den Hostnamen. Der Unterschied liegt darin, dass kein Standarddomainname eingestellt wird. Solange kein Domainname konfiguriert ist oder per DHCP geliefert wurde, bleibt der Domainname leer.

Die Einstellungen zum Domainnamen sind z. B. auf der WBM-Seite „Configuration of Host- and Domain Name“ in der Gruppe „Domain Name“ möglich.

Tabelle 32: WBM-Seite „Configuration of Host- and Domain Name“ – Gruppe „Domain Name“

Parameter	Bedeutung
Currently used	Aktuell verwendeter Domainname
Configured	Optionalen Domainnamen eingeben
[Clear]	Optionalen Domainnamen löschen

### 3.5.1.4 Routing

Der Controller erlaubt im Rahmen der TCP/IP-Konfiguration die Einstellung von statischen Routen, IP-Masquerading und Port-Forwarding. Die Konfiguration von Default-Gateways erfolgt durch den Einsatz von statischen Routen, da das Default-Gateway einen Spezialfall der statischen Route darstellt.

Ein Netzwerkteilnehmer sendet alle Netzwerk-Datenpakete für Systeme außerhalb seines lokalen Netzwerks an ein Gateway. Dieses Gateway ist dafür zuständig, die Datenpakete geeignet weiterzuleiten, sodass sie das Zielsystem erreichen. Um unterschiedliche Zielsysteme erreichen zu können, kann es erforderlich sein, mehrere Gateways zu konfigurieren. Diese Konfiguration erfolgt über das Hinzufügen von Routing-Einträgen. Ein Routing-Eintrag besteht dabei aus der Angabe von:

- Destination-Address
- Destination-Mask
- Gateway-Address
- Gateway-Metric
- Interface

Über die Routing-Einträge wird konfiguriert, an welche Gateways die Netzwerk-Datenpakete gesendet werden. Wird der Controller im Switched-Mode betrieben und besitzt nur ein Netzwerk-Interface, verläuft sämtlicher Netzwerkverkehr über dieses Netzwerk-Interface. Wird der Controller im Separated-Mode betrieben oder enthält der Controller ein Modem, besitzt er mehr als ein Netzwerk-Interface. Damit ist es möglich, dass ein Netzwerk-Datenpaket den Controller auf einem Netzwerk-Interface erreicht und auf einem anderen Netzwerk-Interface wieder verlässt. Diese Weiterleitung zwischen verschiedenen Netzwerk-Interfaces muss explizit freigeschaltet werden und ist im Auslieferungszustand deaktiviert. Um die Weiterleitung zu aktivieren, muss „Enabled“ in der Gruppe „IP Forwarding through multiple interfaces“ aktiviert werden. In diesem Fall kann der Controller als Router fungieren.

Um Netzwerkkommunikation über einen Router weiterzuleiten, ist zu beachten, dass nicht nur der Router sondern auch die jeweiligen Endpunkte der Kommunikation mit entsprechenden Routing-Einträgen versehen werden müssen. Die Routing-Einträge der Endpunkte müssen gewährleisten, dass die gewünschten Netzwerk-Datenpakete sowohl beim Verbindungsaufbau als auch bei den Antworten über den Router gesendet werden.

Die Weiterleitung von IP-Datenpaketen ist z. B. auf der WBM-Seite „Routing“ in der Gruppe „IP Forwarding through multiple interfaces“ einstellbar.

Tabelle 33: WBM-Seite „Routing“ – Gruppe „IP Forwarding through multiple interfaces“

Parameter	Bedeutung
Enabled	Weiterleitung von IP-Datenpaketen zwischen unterschiedlichen Netzwerkschnittstellen erlauben

Parameter	Bedeutung	
	<input type="checkbox"/>	Einstellungen unter „Static Routes“ werden angewendet, ohne dass IP-Datenpakete, die die Steuerung auf einer Netzwerkschnittstelle erreichen, die Steuerung auf einer anderen Netzwerkschnittstelle verlassen dürfen.
	<input checked="" type="checkbox"/>	IP-Pakete dürfen zwischen den Interfaces weitergeleitet werden. Ggf. sind weitere Einstellungen erforderlich.

### 3.5.1.4.1 Statische Routen

Anhand des eingestellten Zielsystems, bestehend aus Destination-Address und Destination-Mask, wird entschieden, an welches Gateway ein Netzwerk-Datenpaket weitergeleitet werden soll. Das Zielsystem kann dabei durch eine einzelne IP-Adresse oder einen IP-Adressbereich angegeben werden. Für ein weiterzuleitendes Netzwerk-Datenpaket wird immer der Routing-Eintrag ausgewählt, welcher die spezifischsten Einträge bzgl. Destination-Address und Destination-Mask aufweist. Das Default-Gateway entspricht dem am wenigsten spezifischen Routing-Eintrag. Alle Netzwerk-Datenpakete zu deren Destination-Address und Destination-Mask kein spezifischer Routing-Eintrag existiert, werden an dieses Default-Gateway geschickt.

#### Default-Gateway

Default-Gateways, auch Default-Routes genannt, werden grundsätzlich in Zusammenhang mit der IP-Konfiguration eingestellt. Jedes Default-Gateway besitzt eine Metrik, die unter allen Default-Gateways eindeutig ist. Bridge <n> besitzt die Metrik 19+<n>. Ein Default-Gateway kann auch über die Routing-Konfiguration definiert werden, z. B. um eine individuelle Metrik zu definieren. Hierzu muss für „Destination-Address“ der Wert „default“ und für Destination-Mask der Wert „0.0.0.0“ gesetzt werden.

#### Route

Wird im Feld „Destination-Address“ eine IP-Adresse oder ein IP-Adressbereich eingetragen, so werden alle Netzwerk-Datenpakete, die an die Netzwerkadresse oder den Netzwerkadressbereich gerichtet sind, an die eingetragene Gateway-Adresse gesendet.

Alternativ kann über das Feld „Interface“ eine Bridge, ein Modem oder ein VPN-Interface angegeben werden, über welches alle Datenpakete, die an die Destination-Address gerichtet sind, geleitet werden. Die Angabe eines Interface ist optional. Es muss jedoch entweder eine Gateway-Adresse, ein Interface oder beides angegeben werden.

Liegt die IP-Adresse des Gateways außerhalb des vom Controller erreichbaren IP-Adressraums, wird die zugehörige Route nicht aktiviert. Dies gilt ebenfalls für Routen, bei denen ein Interface angegeben wird, welches z. B. in der momentanen Bridge-Konfiguration nicht aktiv ist.

Jedem Routing-Eintrag ist eine Metrik zugeordnet. Werden mehrere Routing-Einträge für dieselbe Destination-Address und Destination-Mask eingerichtet, wird über die Metrik eine Priorisierung zwischen den einzelnen Routing-Einträgen vorgegeben. Routing-Einträge mit niedriger Metrik werden in diesem Fall gegenüber Routing-Einträgen mit höherer Metrik bevorzugt. Die Metrik der konfigurierten Routing-Einträge kann für den Controller vorgegeben werden.

Beispiel für Hostroute:

Eine Hostroute bezeichnet eine Route zu einem einzelnen Host. Im nachfolgenden Beispiel soll eine Route zu einem Host mit der IP-Adresse 192.168.1.2 angegeben werden. Die Route verläuft dabei über ein Gateway, welches über die Adresse 10.0.1.3 erreichbar ist. Um auf einem Controller, der in Verbindung zum Gateway steht, eine Hostroute zum Ziel-Host zu konfigurieren, müssen die nachfolgenden Einstellungen vorgenommen werden.

Destination Address:	192.168.1.2	IP-Adresse des Ziel-Hosts
Destination Mask:	255.255.255.255	Subnetzmaske eines einzelnen Hosts
Gateway Address:	10.0.1.3	IP-Adresse des Gateways
Gateway Metric:	20	Priorität der Route

Beispiel für Netzwerkroute:

Eine Netzwerkroute bezeichnet eine Route zu einem Subnetz, welches mehrere Hosts enthalten kann. Im nachfolgenden Beispiel soll eine Route zu einem Subnetz mit der Netzwerkadresse 192.168.1.0 angegeben werden. Die Route verläuft dabei über ein Gateway, welches über die Adresse 10.0.1.3 erreichbar ist. Um auf einem Controller, der in Verbindung zum Gateway steht, eine Netzwerkroute zum Zielnetzwerk zu konfigurieren, müssen die nachfolgenden Einstellungen vorgenommen werden.

Destination Address:	192.168.1.0	IP-Adresse des Zielnetzwerks
Destination Mask:	255.255.255.0	Subnetzmaske des Zielnetzwerks
Gateway Address:	10.0.1.3	IP-Adresse des Gateways
Gateway Metric:	20	Priorität der Route

Beispiel für eine Route über ein Interface:

Im nachfolgenden Beispiel soll eine Route zu einem Host mit der IP-Adresse 192.168.1.2 angegeben werden. Die Route verläuft dabei über das Interface br1, welches der Bridge 2 entspricht. Um auf einem Controller mit einer aktivierten Bridge 2 eine Hostroute zum Ziel-Host über die Bridge 2 zu konfigurieren, müssen die nachfolgenden Einstellungen vorgenommen werden.

Destination Address:	192.168.1.2	IP-Adresse des Ziel-Hosts
Destination Mask:	255.255.255.255	Subnetzmaske eines einzelnen Hosts
Gateway Metric:	20	Priorität der Route
Interface:	br1	Interface, über das das Paket zu leiten ist

Die Einstellungen zu den statischen Routen sind über die WBM-Seite „Routing“ – Gruppe „Custom Routes“ möglich.

Für jede konfigurierte statische Route wird ein eigener Bereich angezeigt. Wenn keine statischen Routen eingetragen wurden, wird „no custom routes“ angezeigt.

Tabelle 34: WBM-Seite „Routing“ – Gruppe „Custom Routes“

Parameter	Bedeutung
Enabled	Verwendung der ausgewählten Route
	<input type="checkbox"/> Die Route wird nicht verwendet.
	<input checked="" type="checkbox"/> Die Route wird verwendet.
Destination Address	Zieladresse des Teilnehmers

Parameter	Bedeutung	
	default	Es sind beliebige Netzwerkteilnehmer erreichbar.
	Netzwerkadresse	Es ist nur ein bestimmter Teilnehmer oder Teilnehmer aus dem vorgegebenen Adress-Pool erreichbar.
Destination Mask	Subnet-Maske des Teilnehmers Wenn bei Destination-Address „default“ eingetragen ist, muss hier der Wert „0.0.0.0“ eingetragen werden.	
Gateway Address	Adresse des Gateways Ist das Eingabefeld „Interface“ leer, ist hier eine Eingabe erforderlich. Wird im Eingabefeld „Interface“ ein Wert eingetragen, ist die Eingabe hier optional.	
Gateway Metric	Metrik der Route Die Metrik bestimmt bei mehreren Routen gleicher Destination-Address und Destination-Mask, an welches Gateway Netzwerk-Datenpakete zuerst geschickt werden. Routen mit kleinerer Metrik werden bevorzugt. Der kleinste Wert ist 0. Der größte Wert ist $2^{32} - 1 = 4.294.967.295$ .	
Interface	Interface, über das die an die Destination-Address gerichteten Pakete geleitet werden Es können sowohl Bridges (br0 ... br3) als auch Modem (wwan0) oder VPN-Interface-Namen verwendet werden. Ist das Eingabefeld „Gateway Address“ leer, ist hier eine Eingabe erforderlich. Wird im Eingabefeld „Gateway Address“ ein Wert eingetragen, ist die Eingabe hier optional.	

### 3.5.1.4.2 Dynamische Routen

Neben den manuell konfigurierbaren Routen können Default-Gateways durch DHCP-Antworten eingestellt werden. Allen per DHCP vergebenen Default-Gateways wird eine eindeutige Metrik zugeordnet.

Die Vergabe der Metrik beginnt bei 10 und erfolgt in Abhängigkeit des Netzwerk-Interface, über das die DHCP-Antwort eingegangen ist. Die Metrik wird aufsteigend, basierend auf der alphanumerischen Sortierung der Netzwerk-Interface-Namen vergeben (z. B. br0, br1, ... wwan0).

Beispiel für Metrik: Ein Controller bezieht seine IP-Konfiguration über einen DHCP-Server und erhält die IP-Adresse sowie Netzwerkmaske 192.168.1.10/24. Außerdem wird manuell ein Gateway mit der IP-Adresse 192.168.1.2 sowie der Metrik 20 auf dem Controller eingerichtet. Der Controller schickt also Netzwerkdatenpakete, für deren Zieladresse kein spezifischer Routing-Eintrag vorhanden ist, an das Gateway 192.168.1.2. Nun wird der DHCP-Server angewiesen, neben IP-Adresse und Netzwerkmaske auch ein Default-Gateway 192.168.1.1 zu verteilen. Dieses Default-Gateway wird vom Controller mit der Metrik 10 versehen. Das über DHCP erhaltene Default-Gateway wird damit gegenüber dem manuell konfigurierten Gateway bevorzugt.

Alle über DHCP empfangenen Default-Gateways werden über die WBM-Seite „Routing“ – Gruppe „Dynamic Routes (assigned by DHCP)“ angezeigt.

Für jede dynamische Route wird ein eigener Bereich angezeigt. Wenn keine dynamischen Routen über DHCP empfangen wurden, wird „no dynamic route“ angezeigt.

Tabelle 35: WBM-Seite „Routing“ – Gruppe „Dynamic Routes (assigned by DHCP)“

Parameter	Bedeutung
Destination Address	Zieladresse des Teilnehmers
Destination Mask	Subnet-Maske des Teilnehmers
Gateway Address	Adresse des Gateways

Parameter	Bedeutung
Gateway Metric	Metrik der Route
Interface	Interface, über das die an die Zieladresse gerichteten Pakete geleitet werden

### 3.5.1.4.3 IP-Masquerading

Der Controller unterstützt neben der Konfiguration von statischen Routen das IP-Masquerading. Dieses kann für ausgewählte Netzwerk-Interfaces des Controllers aktiviert werden. Netzwerk-Datenpakete, die den Controller über ein Netzwerk-Interface verlassen, für das IP-Masquerading aktiviert wurde, erhalten die IP-Adresse des Netzwerk-Interfaces als Absenderadresse. Werden Netzwerk-Datenpakete über den Controller weitergeleitet, wird das hinter dem Controller liegende Netzwerk unter einer einzigen Adresse verborgen.

Tabelle 36: WBM-Seite „Routing“ – Gruppe „IP Masquerading“

Parameter	Bedeutung
Enabled	IP-Masquerading verwenden
	<input type="checkbox"/> IP-Masquerading wird nicht verwendet.
	<input checked="" type="checkbox"/> IP-Masquerading wird verwendet.
Interface	Einen der angegebenen Namen eines Netzwerk-Interface auswählen Über die Auswahl von „other“ ist ein beliebiger Netzwerk-Interface-Name möglich.

### 3.5.1.4.4 Port-Forwarding

Der Controller erlaubt ebenfalls die Konfiguration von Port-Forwarding-Einträgen. Beim Port-Forwarding werden die Destination-Adresse und ggf. der Destination-Port eines Netzwerk-Datenpakets überschrieben, welches den Controller über ein zuvor konfiguriertes Netzwerk-Interface erreicht hat. Somit ist eine Weiterleitung von Netzwerk-Datenpaketen über den Controller an andere Adressen und Ports möglich. Die Weiterleitung kann für die Protokolle UDP und TCP konfiguriert werden.

Tabelle 37: WBM-Seite „Routing“ – Gruppe „Port Forwarding“

Parameter	Bedeutung
Enabled	Port-Forwarding verwenden
	<input type="checkbox"/> Port-Forwarding wird nicht verwendet.
	<input checked="" type="checkbox"/> Port-Forwarding wird verwendet.
Interface	Einen der angegebenen Namen eines Netzwerk-Interface auswählen Über die Auswahl von „other“ ist ein beliebiger Netzwerk-Interface-Name möglich.
Port	Port auswählen, auf dem weiterzuleitende Netzwerk-Datenpakete das Produkt erreichen
Protocol	Protokoll auswählen, welches für das Port-Forwarding berücksichtigt werden soll; Zur Auswahl stehen TCP, UDP oder beide Protokolle.
Destination Address	Netzwerkadresse des Zielteilnehmers auswählen Diese Adresse ersetzt die ursprüngliche Destination-Adresse des Netzwerk-Datenpakets.
Destination Port	Port-Nummer des Zielteilnehmers auswählen Dieser Wert ersetzt den ursprünglichen Destination-Port des Netzwerk-Datenpakets.

## 3.5.2 Netzwerksicherheit

### 3.5.2.1 Benutzer und Passwörter

Es gibt verschiedene Gruppen von Benutzern, die für unterschiedliche Dienste verwendet werden können.

Bei allen Benutzern sind Standardpasswörter eingestellt. Es wird dringend empfohlen, diese bei der Inbetriebnahme zu ändern!

#### Hinweis

##### Passwörter ändern!

Die im Auslieferungszustand eingestellten Standardpasswörter sind in dieser Betriebsanleitung dokumentiert und bieten so keinen hinreichenden Schutz.

- Ändern Sie die Passwörter entsprechend Ihren Erfordernissen.

##### Dienste und Benutzer

In der folgenden Tabelle sind alle passwortgeschützten Dienste und die dazugehörigen Benutzer aufgelistet.

Tabelle 38: Dienste und Benutzer

Dienst	Benutzer			SNMP
	Linux®			
	root	admin	user	
Web-Based-Management (WBM)	X	X	X	
Linux®-Konsole	X	X	X	
Console-Based-Management (CBM)	X			
CODESYS		X		
FTP	X	X	X	
FTPS	X	X	X	
SSH	X	X	X	
SNMP				X

##### Linux®-Benutzergruppe

Die Gruppe der Linux®-Benutzer umfasst die eigentlichen Benutzer des Betriebssystems, die von den meisten Services ebenfalls verwendet werden.

Tabelle 39: Linux®-Benutzer

Benutzer	Besonderheit	Home-Verzeichnis	Standardpasswort
root	Superuser	/root	wago
admin	CODESYS Benutzer	/home/admin	wago
user	Einfacher Benutzer	/home/user	user

Die Passwörter für diese Benutzer können über das WBM oder über eine Terminalverbindung konfiguriert werden.

**i Hinweis****Passwörter ändern!**

Die im Auslieferungszustand eingestellten Standardpasswörter sind in dieser Betriebsanleitung dokumentiert und bieten so keinen hinreichenden Schutz.

- Ändern Sie die Passwörter entsprechend Ihren Erfordernissen.

**i Hinweis****Zulässige Zeichen für Passwörter**

Passwörter dürfen nur die folgenden Zeichen enthalten:

Kleinbuchstaben (a ... z), Großbuchstaben (A ... Z), Ziffern (0 ... 9) und Sonderzeichen (! " # \$ % & ' ( ) \* + , . / : ; < = > ? @ [ ] ^ \_ ` { } | ~ -).

**i Hinweis****Passwortlänge beachten!**

Für CODESYS muss die Passwortlänge größer gleich 1 Zeichen und kleiner 60 Zeichen sein!

Für den angemeldeten Linux®-Benutzer kann das Passwort über die WBM-Seite „WBM User Configuration“ in der Gruppe „Change Passwords“ geändert werden.

Tabelle 40: WBM-Seite „WBM User Configuration“ – Gruppe „Change Passwords“

Parameter	Bedeutung
Old Password	Aktuell verwendetes Passwort zur Authentifizierung eingeben.
New Password	Neues Passwort eingeben.
Confirm Password	Neues Passwort zur Kontrolle erneut eingeben.

**SNMP-Benutzergruppe**

Der SNMP-Dienst verwaltet seine eigenen Benutzer. Hier sind im Auslieferungszustand keine Benutzer hinterlegt.

**3.5.2.2 Webserverauthentifizierung**

Die WBM-Seiten können wahlweise mit dem Webprotokoll HTTP oder HTTPS geöffnet werden. HTTPS sollte bevorzugt verwendet werden, da es das TLS-Protokoll einsetzt. Das TLS-Protokoll sichert die Kommunikation durch Verschlüsselung und Authentifizierung.

Die Standardeinstellung des Controllers ermöglicht starke Verschlüsselung, nutzt aber nur einfache Authentifizierungsverfahren.

Da eine Authentifizierung für alle sicheren Kommunikationskanäle eine zentrale Rolle spielt, ist dringend angeraten, eine sicherere Authentifizierung durchzuführen.

Basis der Authentifizierung bildet das auf dem Controller gespeicherte Sicherheitszertifikat. Im Auslieferungszustand verwendet der Controller ein generisches Sicherheitszertifikat im x509-Format.

Um eine sicherere Authentifizierung zu ermöglichen, müssen Sie ein spezifisches, für das individuelle Gerät erstellte Zertifikat installieren.

Speichern Sie das individuelle Zertifikat unter folgendem Pfad auf dem Gerät: `/etc/lighttpd/custom-cert.pem`.

Nach einem Neustart des Webservers wird das individuelle Zertifikat aktiv.

Wenn das individuelle Zertifikat vom Gerät gelöscht wird, verwendet der Webserver nach einem Neustart wieder das generische Sicherheitszertifikat.

### 3.5.2.2.1 TLS-Verschlüsselung

Beim Aufbau einer HTTPS-Verbindung handeln der Webbrowser und der Webserver aus, welche TLS-Version und welches kryptografische Verfahren verwendet wird.

Die erlaubten TLS-Versionen und kryptografische Verfahren sind einstellbar („Strong“/„Extended Compatibility“).

Mit der Einstellung „Strong“ erlaubt der Webserver nur TLS 1.3 und starke Algorithmen. Ältere Software und ältere Betriebssysteme unterstützen eventuell TLS 1.3 und die Verschlüsselungsalgorithmen nicht.

Mit der Einstellung „Extended Compatibility“ ist auch TLS 1.2 mit weniger starken kryptografischen Verfahren erlaubt. Eine Verwendung wird nur für die Abwärtskompatibilität mit älteren Systemen empfohlen.

#### Hinweis

##### Technische Richtlinie TR-02102 des BSI

Die Regeln für die TLS-Einstellungen richten sich nach der technischen Richtlinie TR-02102 des Bundesamtes für Sicherheit in der Informationstechnik.

Die Richtlinie finden Sie unter: [www.bsi.bund.de](https://www.bsi.bund.de).

Die bei HTTPS erlaubten kryptografischen Verfahren und die benutzbaren TLS-Versionen können in der Gruppe „TLS Configuration“ der WBM-Seite „Security Settings“ umgeschaltet werden.

Tabelle 41: WBM-Seite „Security Settings“ – Gruppe „TLS Configuration“

Parameter	Bedeutung
TLS Configuration	Erlaubte TLS-Versionen und kryptografischen Verfahren für HTTPS einstellen
Extended Compatibility	Der Webserver erlaubt TLS 1.3 und auch TLS 1.2 mit weniger starken kryptografischen Verfahren.
Strong	Der Webserver erlaubt nur TLS 1.3 und starke Algorithmen.

### 3.5.2.3 Root-Zertifikate

Bei mittels TLS verschlüsselter Kommunikation werden zur Überprüfung der Authentizität des Kommunikationspartners Root-Zertifikate verwendet.

Ein Root-Zertifikat, welches von einer Zertifizierungsstelle signiert wurde, dient dazu, die Gültigkeit aller Zertifikate zu verifizieren, die von dieser Zertifizierungsstelle ausgestellt wurden.

Die Basis für die Authentifizierung von im Internet gehosteten Diensten (z. B. E-Mail-Provider, Cloud-Dienste) bilden die auf dem Controller gespeicherten Root-Zertifikate (Root-CA-Bundle).

Der Standardablageort der Root-Zertifikate ist: `/etc/ssl/certs/ca-certificates.crt`.

Die Datei beinhaltet die von Mozilla bereitgestellten Zertifikate. Eine Liste mit den inkludierten Root-Zertifikaten und der jeweiligen Gültigkeitsdauer kann unter folgender Adresse abgefragt werden:

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

Die Root-Zertifikate können durch Aktualisierung der Datei `/etc/ssl/certs/ca-certificates.crt` auf dem Controller aktualisiert werden.

### Sehen Sie dazu auch

- 📖 Root-Zertifikate aktualisieren [▶ 101]

## 3.5.2.4 Firewall

### 3.5.2.4.1 Globale Firewall-Einstellungen

Tabelle 42: WBM-Seite „General Firewall Configuration“ – Gruppe „Global Firewall Parameter“

Parameter	Bedeutung
Firewall enabled entirely	Komplette Funktionalität der Firewall aktivieren/deaktivieren Diese Einstellung hat oberste Priorität. Ist die Firewall ausgeschaltet, haben alle anderen Einstellungen keine direkte Auswirkung. Die Konfiguration der anderen Parameter ist trotzdem möglich, damit die Firewall-Parameter korrekt eingestellt werden können, bevor die Firewall aktiviert wird. Diese Einstellung ist unabhängig von der Einstellung zu „Filter enabled“ in der Gruppe „MAC address filter state Bridge <n>“ auf der Seite „MAC address filter state Bridge“.
ICMP echo broadcast protection	„ICMP echo broadcast“-Schutz aktivieren/deaktivieren
Max. UDP connections per second	Maximale Anzahl der UDP-Verbindungen pro Sekunde eingeben
Max. TCP connections per second	Maximale Anzahl der TCP-Verbindungen pro Sekunde eingeben

### Hinweis

#### **CODESYS Dienste werden bei eingeschalteter Firewall ohne User-Filter abgewiesen!**

Wenn CODESYS Dienste (z. B. Modbus, OPC-UA, SNMP oder IIOT) genutzt werden, müssen in der Firewall-Konfiguration User-Filter für diese Dienste angelegt werden. Die User-Filter müssen so konfiguriert sein, dass die entsprechenden Ports akzeptiert werden.

### 3.5.2.4.2 Schnittstellenbezogene Firewall-Einstellungen

Tabelle 43: WBM-Seite „Interface Configuration“ – Gruppe „Firewall Configuration Bridge <n> / VPN / WAN“

Parameter	Bedeutung
Firewall enabled for Interface	Firewall für die jeweilige Schnittstelle aktivieren/deaktivieren
ICMP echo protection	„ICMP echo“-Schutz für die jeweilige Schnittstelle aktivieren/deaktivieren
ICMP echo limit per second	Maximale Anzahl „ICMP pings“ pro Sekunde eingeben. „0“ = „Disabled“
ICMP burst limit (0=disabled)	Maximale Anzahl „ICMP echo burst“ pro Sekunde eingeben
Service Configuration	Firewall für den jeweiligen Dienst aktivieren/deaktivieren
FTP/FTPES	Nicht jeder der hier gezeigten Dienste ist für jedes Produkt verfügbar.

Parameter	Bedeutung
FTPS (implicit)	Die Dienste selber müssen über die Seite „Ports and Services“ gesondert ein und ausgeschaltet werden.
HTTP	
HTTPS	
I/O Check	
PLC Runtime	
WebVisu – HTTP (port 8080)	
WebVisu – HTTPS (port 8081)	
SSH	
SNMP	
OPC UA (port 4840)	
BACnet (port 47808)	
PROFINET IO	
DNP3 (port 20000)	
IEC60870-5-104 (port 2404)	
IEC61850 (port 102)	

Auf Controllern mit Telecontrol-Funktionalität werden standardmäßig die in der nachfolgenden Tabelle aufgelisteten Firewall-Ports geöffnet. Über diese Ports können die entsprechenden Telecontrol-Dienste ausgeführt werden, ohne dass deren Kommunikation durch die Firewall blockiert wird.

Tabelle 44: Ports für Telecontrol-Funktionalität

Protokoll	Port
DNP3	20000
IEC60870-5-104	2404
IEC61850	102

### 3.5.2.4.3 MAC-Adressenfilter

#### Globale Einstellung

Tabelle 45: WBM-Seite „Configuration of MAC address filter“ – Gruppe „Global MAC address filter state“

Parameter	Bedeutung
Filter enabled	Globalen MAC-Adressenfilter aktivieren/deaktivieren

#### Bridge-bezogene Einstellung

Tabelle 46: WBM-Seite „Configuration of MAC address filter“ – Gruppe „MAC address filter state Bridge <n>“

Parameter	Bedeutung
Filter enabled	MAC-Adressenfilter für die jeweilige Bridge aktivieren/deaktivieren; Diese Einstellung ist unabhängig von der Einstellung zu „Firewall enabled entirely“ in der Gruppe „Global Firewall Parameter“ auf der Seite „General Firewall Configuration“.

#### MAC-Adressenfilter-Whitelist

Die „MAC Address Filter Whitelist“ enthält zwei Default-Einträge mit folgenden Werten:

- Beschreibung: All WAGO devices  
MAC-Adresse: 00:30:DE:00:00:00  
MAC-Mask: ff:ff:ff:00:00:00
- Beschreibung: Enable docker bridges  
MAC-Adresse: 02:42:00:00:00:00

MAC-Mask: ff:ff:00:00:00:00

Wenn Sie den ersten Default-Eintrag freischalten, können bereits verschiedene WAGO Produkte im Netzwerk untereinander kommunizieren.

Für jeden konfigurierten Filter wird ein eigener Bereich angezeigt.

Wenn kein MAC-Address-Filter angelegt wurde, wird „no MAC Address filters“ angezeigt.

Im Bereich „Add filter to whitelist“ können maximal 10 MAC-Address-Filter angelegt werden.

Tabelle 47: WBM-Seite „Configuration of MAC address filter“ – Gruppe „MAC address filter whitelist“

Parameter	Bedeutung
Description	Beschreibung der Geräte bzw. Bereiche, die bei generell aktivierter Firewall durch das Aktivieren des Filters freigeschaltet werden können. Die Beschreibung ist nur bei den initial in der Werkseinstellung vorhandenen Einträgen sichtbar.
MAC address	MAC-Adresse des Listeneintrags
MAC mask	MAC-Maske des Listeneintrags
Filter enabled	Filter für den Listeneintrag aktivieren/deaktivieren

#### 3.5.2.4.4 User-Filter

Für jeden konfigurierten Filter wird ein eigener Bereich angezeigt.

Wenn kein User-Filter angelegt wurde, wird „no user filters“ angezeigt.

Im Bereich „Add new user filter“ können maximal 10 User-Filter angelegt werden.

Es müssen nur Werte in die Felder eintragen werden, die beim Filter gesetzt werden sollen.

Mindestens 1 Wert muss eingetragen werden, alle anderen Felder können leer bleiben.

Tabelle 48: WBM-Seite „Configuration of User Filter“ – Gruppe „User filter“

Parameter	Bedeutung	
Policy	Netzwerkteilnehmer durch den Filter zulassen/ausschließen	
	Allow	Der Netzwerkteilnehmer ist zugelassen.
	Drop	Der Netzwerkteilnehmer ist ausgeschlossen.
Source IP address	Quell-IP-Adresse für den Filter	
Source Netmask	Quellnetzmaske für den Filter	
Source Port	Quell-Port-Nummer für den Filter	
Destination IP address	Ziel-IP-Adresse für den Filter	
Destination Netmask	Zielnetzmaske für den Filter	
Destination Port	Ziel-Port-Nummer für den Filter	
Protocol	Protokolle für den Filter	
	TCP/UDP	Der TCP-Service und der UDP-Service werden gefiltert.
	TCP	Der TCP-Service wird gefiltert.
UDP	Der UDP-Service wird gefiltert.	
Input Interface	Schnittstellen für den Filter	
	Any	Alle Schnittstellen werden gefiltert.
	Bridge <n>	Die zur Bridge <n> zugeordneten Schnittstellen werden gefiltert. Es werden nur die konfigurierten Bridges angezeigt.
VPN	Die VPN-Schnittstelle wird gefiltert.	

** Hinweis****CODESYS Dienste werden bei eingeschalteter Firewall ohne User-Filter abgewiesen!**

Wenn CODESYS Dienste (z. B. Modbus, OPC-UA, SNMP oder IIOT) genutzt werden, müssen in der Firewall-Konfiguration User-Filter für diese Dienste angelegt werden. Die User-Filter müssen so konfiguriert sein, dass die entsprechenden Ports akzeptiert werden.

### 3.5.3 Netzwerkdienste

#### 3.5.3.1 DHCP-Client

Der Controller kann über den DHCP-Client Netzwerkparameter von einem externen DHCP-Server beziehen.

Folgende Parameter können bezogen werden:

- IP-Adresse
- Subnetzmaske
- Router/Gateway
- Hostname
- Domain
- DNS-Server
- NTP-Server

Für die Parameter IP-Adresse, Subnetzmaske und Router/Gateway werden die Einträge pro ETHERNET-Schnittstelle gespeichert.

Bei mehreren Netzwerkschnittstellen mit DHCP wird der Hostname von der Netzwerkschnittstelle (Bridge oder Wwan) mit der höchsten Priorität übernommen. Die Priorität ist alphanumerisch durch den Namen der Netzwerkschnittstelle festgelegt. Somit hat die Bridge1 die höchste Priorität gefolgt von Bridge2, Bridge3, ..., Wwan0.

#### 3.5.3.2 DHCP-Server

Für die automatische Konfiguration von IP-Adressen von Netzwerkteilnehmern am gleichen Subnetz bietet der Controller den DHCP-Server-Dienst an. Üblicherweise darf zu einer Zeit immer nur ein DHCP-Server an einem Subnetz aktiv sein.

Für den DHCP-Server ist einstellbar:

- der Dienst selbst (aktiv/nicht aktiv)
- der Bereich der dynamisch zu vergebenden IP-Adressen
- die Gültigkeitsdauer (Lease Time) der dynamisch vergebenen IP-Adressen
- eine Liste mit statischen Zuordnungen von IP-Adressen zu MAC-Adressen

Im „Switched“ Modus sind diese Einstellungen für beide Schnittstellen gemeinsam und im „Separated“ Modus für jede Schnittstelle getrennt möglich.

Neben der IP-Adresse übergibt der DHCP-Server noch weitere Parameter. Die nachfolgende Tabelle zeigt die komplette Liste.

Tabelle 49: Liste der per DHCP übertragenen Parameter

Parameter	Bedeutung
IP-Adresse	Eine IP-Adresse aus dem Bereich der zulässigen Adressen; dieser Bereich kann im WBM konfiguriert werden. Der DHCP-Server ermittelt aus der MAC-Adresse des anfragenden Netzwerkteilnehmers (Client) und dem Bereich der zu vergebenden Adressen die IP-Adresse, die dem Netzwerkteilnehmer übergeben wird. Solange der konfigurierte Adressbereich nicht geändert wird und keine Engpässe bei der Vergabe von IP-Adressen auftreten, wird der DHCP-Server den anfragenden Netzwerkteilnehmern immer wieder die gleichen IP-Adressen zuordnen. Meldet sich ein Netzwerkteilnehmer, für dessen MAC-Adresse eine feste IP-Adresse im WBM konfiguriert wurde, wird ihm diese Adresse übergeben. Eine solcherart fest zugeordnete IP-Adresse kann auch außerhalb des Bereichs der frei vergebbaren IP-Adressen liegen. Anstelle der MAC-Adresse zur Identifizierung des anfragenden Netzwerkteilnehmers kann auch ein Hostname angegeben werden.
Subnetzmaske	Die in den Netzwerkeinstellungen des DHCP-Servers konfigurierte Subnetzmaske für das betroffene lokale Netzwerk wird übertragen. Subnetzmaske und IP-Adresse bestimmen den Bereich der im lokalen Netzwerk gültigen IP-Adressen.
Broadcast-Adresse	IP-Adresse, mit der ein IP-Paket gleichzeitig an alle Netzwerkteilnehmer am Subnetz gesendet werden kann.
Lease-Time	Bestimmt die Gültigkeitsdauer der einem Netzwerkteilnehmer übergebenen DHCP-Parameter; der Netzwerkteilnehmer ist per Protokoll verpflichtet, nach der halben Gültigkeitsdauer die Netzwerkeinstellung erneut anzufagen. Die Lease-Time wird im WBM konfiguriert.
Hostname	Der Netzwerkname wird dem Netzwerkteilnehmer übergeben. Üblicherweise sendet der Netzwerkteilnehmer mit seiner Anfrage nach der IP-Adresse seinen eigenen Namen mit. Dieser wird dann vom DHCP-Server in seiner Antwort verwendet.
Name-Server	Der DHCP-Server übergibt seine eigene IP-Adresse als DNS-Name-Server an den Netzwerkteilnehmer.
Default-Gateway	Der DHCP-Server übergibt seine eigene IP-Adresse als Default-Gateway an den Netzwerkteilnehmer. Das Default-Gateway wird benötigt, um mit Teilnehmern außerhalb des lokalen Netzwerks zu kommunizieren.

Nicht alle Parameter sind im WBM einstellbar. Wenn für die vorhandenen Parameter andere Werte eingestellt oder weitere Parameter per DHCP übertragen werden sollen, muss der DHCP-Server manuell konfiguriert werden. Beim Controller wird der DHCP-Server-Dienst vom Programm „dnsmasq“ übernommen.

Zur Einstellung der Konfiguration ist per Linux®-Kommandozeile mit einem Editor die Datei „/etc/dnsmasq.d/dnsmasq\_default.conf“ anzupassen.

Die Einstellungen erfolgen z. B. im WBM über die Seite „DHCP Configuration“.

Tabelle 50: WBM-Seite „DHCP Server Configuration“ – Gruppe „DHCP Server Configuration Bridge <n>“

Parameter	Bedeutung
Service active	DHCP-Server-Dienst für die Bridge <n> aktivieren/deaktivieren;
	<input type="checkbox"/> Der DHCP-Server-Dienst für die Bridge <n> ist nicht aktiviert.
	<input checked="" type="checkbox"/> Der DHCP-Server-Dienst für die Bridge <n> ist aktiviert.
Start IP for Range	Anfangswert des verfügbaren IP-Adressbereichs eingeben.
End IP for Range	Endwert des verfügbaren IP-Adressbereichs eingeben.
Lease time (min)	Ausleihzeit in Minuten eingeben. Werkseinstellung: 120 Minuten
Static Hosts	Statische Zuordnungen von MAC-IDs oder Hostnamen zu IP-Adressen; Wenn keine Zuordnung vorhanden ist, wird „No static hosts configured“ angezeigt.
Add Static Host	Statische Zuordnungen von MAC-Adressen oder Hostnamen zu IP-Adressen hinzufügen; Es sind max. 15 Zuordnungen möglich.

Parameter	Bedeutung
MAC Address or Hostname	MAC-Adresse oder Hostnamen eingeben; Z. B. „01:02:03:04:05:06=192.168.1.20“ oder „hostname=192.168.1.20“.
IP Address	IP-Adresse eingeben.

### 3.5.3.3 DNS-Server

Für die automatische Zuordnung von Hostnamen zu IP-Adressen von Netzwerkteilnehmern bietet der Controller den DNS-Server-Dienst an. Der DNS-Server übernimmt vom DHCP-Server die Namen und IP-Adressen von lokalen Netzwerkteilnehmern. Anfragen für nichtlokale Namen, beispielsweise aus dem Internet, leitet dieser DNS-Server an übergeordnete DNS-Server weiter, sofern ein solcher konfiguriert und erreichbar ist.

Für den DNS-Server ist einstellbar:

- der Dienst selbst (aktiv/nicht aktiv)
- die Zugriffsart auf die Zuordnungen  
 Im „Proxy“-Modus werden die Anfragen zwischengespeichert (durchsatzoptimiert).  
 Im Relay-Modus werden die Anfragen direkt an übergeordnete Name-Server weitergeleitet.
- eine Liste mit maximal 15 statischen Zuordnungen von IP-Adressen zu Hostnamen  
 Wenn nur der Hostname verwendet wird, so wird automatisch der Hostname mit dem konfigurierten Domainnamen bzw. dem Default-Domainnamen expandiert, um eine FQDN-Namensauflösung sicherzustellen.

Die Einstellungen erfolgen z. B. im WBM über die Seite „Configuration of DNS Service“.

Tabelle 51: WBM-Seite „Configuration of DNS Server“ – Gruppe „DNS Server“

Parameter	Bedeutung
Service active	DNS-Server-Dienst aktivieren/deaktivieren;
	<input type="checkbox"/> Der DNS-Server-Dienst ist deaktiviert.
	<input checked="" type="checkbox"/> Der DNS-Server-Dienst ist aktiviert.
Mode	Betriebsart einstellen;
	Proxy Anfragen werden zur Durchsatzoptimierung zwischengespeichert.
	Relay Alle Anfragen werden direkt weitergeleitet.
Static Hosts	Statische Zuordnungen von Hostnamen zu IP-Adressen; Wenn keine Zuordnung vorhanden ist, wird „No static hosts configured“ angezeigt.
Add Static Host	Statische Zuordnungen von IP-Adressen zu Hostnamen hinzufügen; Es sind max. 10 Zuordnungen möglich.
IP Address	IP-Adresse eingeben; Z. B. „192.168.1.20:hostname“
Hostname	Hostnamen eingeben.

### 3.5.3.4 SNMP

SNMP (Simple-Network-Management-Protokoll) ist ein Standardprotokoll zur Überwachung und für das Management von Geräten in einem TCP/IP-Netzwerk. Es dient dem Transport von Kontrolldaten, die den Austausch von Management-Informationen, Status- und Statistikdaten zwischen einzelnen Netzwerkkomponenten und einem Management-System ermöglichen.

Das Protokoll steht in der Version v1, v2c und v3 zur Verfügung. Die Versionen sind unabhängig voneinander und können parallel oder auch einzeln aktiviert und verwendet werden.

Allgemeine Einstellungen für SNMP sind z. B. über die WBM-Seite „Configuration of general SNMP parameters“ möglich.

Tabelle 52: WBM-Seite „Configuration of general SNMP parameters“ – Gruppe „General SNMP Configuration“

Parameter	Bedeutung
Service active	SNMP-Dienst aktivieren/deaktivieren;
	<input type="checkbox"/> Der SNMP-Dienst ist deaktiviert.
	<input checked="" type="checkbox"/> Der SNMP-Dienst ist aktiviert.
Name of Device	Produktname (sysName) eingeben.
Description	Produktbeschreibung (sysDescription) eingeben.
Physical Location	Standort des Produktes (sysLocation) eingeben.
Contact	E-Mail-Kontaktadresse (sysContact) eingeben.
ObjectID	Object-ID eingeben.

#### 3.5.3.4.1 SNMP v1/v2c

SNMP v1 und v2c ist ein Community-Nachrichtenaustausch innerhalb einer Netzgemeinschaft mit einem gemeinsamen Community-Namen.

Über den Community-Namen können Beziehungen zwischen SNMP-Managern (Trap-Empfänger) und -Agenten eingerichtet werden, die jeweils als Community bezeichnet werden. Die Communities steuern die Identifizierung sowie den Zugriff zwischen den SNMP-Teilnehmern. Der Community-Name kann durch den Trap-Empfänger ausgewertet werden.

Um das SNMP-Protokoll verwenden zu können, muss immer ein gültiger Community-Name angegeben sein.

Der Community-Name darf maximal 32 Zeichen lang sein und keine Leerzeichen enthalten. Der Standardwert ist „public“.

Die Zugriffsrechte für die Community und die SNMP-Version, über welche die Traps gesendet werden sollen, sind einstellbar.

Einstellungen für die SNMP-v1/v2c-Parameter sind z. B. über die WBM-Seite „Configuration of SNMP v1/v2c Parameters“ möglich.

#### Communities

Für jede konfigurierte Community wird ein eigener Bereich „Community <n>“ angezeigt. Wenn keine Community konfiguriert wurde, wird „(no Communities configured)“ angezeigt.

In Bereich „Add new Community“ können Sie eine neue Community hinzufügen.

Tabelle 53: WBM-Seite „Configuration of SNMP v1/v2c Parameters“ – Gruppe „Communities“

Parameter	Bedeutung
Name	Community-Name für die SNMP-Manager-Konfiguration
Access	Zugriffsrechte für die Community; Mögliche Werte sind: <ul style="list-style-type: none"> <li>• ReadOnly</li> <li>• ReadWrite</li> </ul>

### Trap-Receiver

Für jeden konfigurierten Trap-Empfänger wird ein eigener Bereich „Trap Receiver <n>“ angezeigt.

Wenn kein Trap- Empfänger konfiguriert wurde, wird „(no Trap Receivers configured)“ angezeigt.

Im Bereich „Add new Trap Receiver“ können Sie einen neuen Trap-Empfänger anlegen.

Tabelle 54: WBM-Seite „Configuration of SNMP v1/v2cparameters“ – Gruppe „Trap Receivers“

Parameter	Bedeutung
Host	Hostname oder IP-Adresse des Trap-Empfängers (Managementstation)
Community Name	Community-Name für die Trap-Empfänger-Konfiguration
Version	SNMP-Version, über welche die Traps gesendet werden sollen; Mögliche Werte sind: <ul style="list-style-type: none"> <li>▪ v1</li> <li>▪ v2c</li> </ul>

#### 3.5.3.4.2 SNMP v3

SNMP v3 wird in sicherheitsrelevanten Netzwerken eingesetzt. Die Nutzdaten der SNMP-Nachrichten können verschlüsselt übertragen und angefragte und zu schreibende Werte nicht über ETHERNET mitgehört werden.

Es ist möglich, eine Passwort-Authentifizierung und einen Verschlüsselungscode zu konfigurieren.

Der Benutzername muss eindeutig sein, ein bereits vorhandener Benutzername wird bei der Neueingabe nicht akzeptiert.

Der Benutzername muss mindestens 8 Zeichen lang sein und darf maximal 32 Zeichen lang sein.

Der Benutzername darf Kleinbuchstaben (a ... z), Großbuchstaben (A ... Z), Ziffern (0 ... 9), Sonderzeichen (! () \* ~ ' . - \_) aber keine Leerzeichen enthalten.

Das Passwort (Authentication Key) und der Verschlüsselungscode (Privacy Key) müssen mindestens 8 Zeichen lang sein und dürfen maximal 32 Zeichen lang sein.

Das Passwort und der Verschlüsselungscode dürfen Kleinbuchstaben (a ... z), Großbuchstaben (A ... Z), Ziffern (0 ... 9), Sonderzeichen (! () \* ~ ' . - \_) aber keine Leerzeichen enthalten.

Einstellungen für die SNMP-v3-Parameter sind z. B. über die WBM-Seite „Configuration of SNMP v3 Parameters“ möglich.

### User

Für jeden konfigurierten v3-User wird ein eigener Bereich „User <n>“ angezeigt.

Wenn kein v3-User konfiguriert wurde, wird „(no Users configured)“ angezeigt.

Im Bereich „Add new v3 User“ können Sie einen neuen v3-User anlegen.

Sie können maximal 10 User anlegen.

Tabelle 55: WBM-Seite „Configuration of SNMP v3 Parameters“ – Gruppe „Users“

Parameter	Bedeutung
Security Authentication Name	Benutzername

Parameter	Bedeutung
Authentication Type	Authentifizierungstyp für die SNMP-v3-Pakete; Mögliche Werte sind: <ul style="list-style-type: none"> <li>Keine Authentifizierung („None“)</li> <li>Message Digest 5 („MD5“)</li> <li>Secure Hash Algorithm („SHA“, „SHA224“, „SHA256“, „SHA384“, „SHA512“)</li> </ul>
Authentication Key	Passwort für die Authentifizierung
Privacy	Verschlüsselungsalgorithmus für die SNMP-Nachricht; Mögliche Werte sind: <ul style="list-style-type: none"> <li>Keine Verschlüsselung („None“)</li> <li>Data Encryption Standard („DES“)</li> <li>Advanced Encryption Standard („AES“, „AES128“, „AES192“, „AES192C“, „AES256“, „AES256C“)</li> </ul>
Privacy Key	Verschlüsselungscode
Access	Zugriffsrechte für den v3-User; Mögliche Werte sind <ul style="list-style-type: none"> <li>ReadOnly</li> <li>ReadWrite</li> </ul>

### Trap-Receiver

Für jeden konfigurierten v3-Trap-Empfänger wird ein eigener Bereich „Trap Receiver <n>“ angezeigt.

Wenn kein v3-Trap-Empfänger konfiguriert wurde, wird „(no Trap Receivers configured)“ angezeigt.

Im Bereich „Add new Trap Receiver“ können Sie einen neuen v3-Trap-Empfänger anlegen. Sie können maximal 10 Trap-Empfänger anlegen.

Tabelle 56: WBM-Seite „Configuration of SNMP v3 Parameters“ – Gruppe „Trap Receivers“

Parameter	Bedeutung
Security Authentication Name	Benutzername
Authentication Type	Authentifizierungstyp für die SNMP-v3-Pakete; Mögliche Werte sind: <ul style="list-style-type: none"> <li>Keine Authentifizierung („None“)</li> <li>Message Digest 5 („MD5“)</li> <li>Secure Hash Algorithm („SHA“, „SHA224“, „SHA256“, „SHA384“, „SHA512“)</li> </ul>
Authentication Key	Passwort für die Authentifizierung
Privacy	Verschlüsselungsalgorithmus für die SNMP-Nachricht; Mögliche Werte sind: <ul style="list-style-type: none"> <li>Keine Verschlüsselung („None“)</li> <li>Data Encryption Standard („DES“)</li> <li>Advanced Encryption Standard („AES“, „AES128“, „AES192“, „AES192C“, „AES256“, „AES256C“)</li> </ul>
Privacy Key	Verschlüsselungscode
Host	Hostname oder IP-Adresse des v3-Trap-Empfängers

### 3.5.3.5 FTP/FTPES

Tabelle 57: WBM-Seite „Configuration of Network Services“ – Gruppe „FTP“

Parameter	Bedeutung
Service active	FTP-Service aktivieren/deaktivieren;
	<input type="checkbox"/> Der FTP-Service ist deaktiviert; Werkseinstellung

Parameter	Bedeutung	
	<input checked="" type="checkbox"/>	Der FTP-Service ist aktiviert.

Tabelle 58: WBM-Seite „Configuration of Network Services“ – Gruppe „FTPES (explicit FTPS)“

Parameter	Bedeutung	
Service active	FTPES (explicit FTPS)-Service aktivieren/deaktivieren;	
	<input type="checkbox"/>	Der FTPES-Service ist deaktiviert; Werkseinstellung
	<input checked="" type="checkbox"/>	Der FTPES-Service ist aktiviert.

### 3.5.3.6 HTTP/HTTPS

Tabelle 59: WBM-Seite „Configuration of Network Services“ – Gruppe „HTTP“

Parameter	Bedeutung	
Service active	HTTP-Service aktivieren/deaktivieren;	
	<input type="checkbox"/>	Der HTTP-Service ist deaktiviert; Werkseinstellung
	<input checked="" type="checkbox"/>	Der HTTP-Service ist aktiviert.

Tabelle 60: WBM-Seite „Configuration of Network Services“ – Gruppe „HTTPS“

Parameter	Bedeutung	
Service active	Status des HTTPS-Service	
	<input type="checkbox"/>	Der HTTPS-Service ist deaktiviert.
	<input checked="" type="checkbox"/>	Der HTTPS-Service ist aktiviert.

### 3.5.3.7 I/O-CHECK

#### Hinweis

#### Nicht benötigte Ports und Dienste schließen!

Durch geöffnete Ports können Unbefugte Zugriff auf Ihr Automatisierungssystem erhalten.

- Um die Gefahr von Cyberangriffen zu verringern und damit die Cyber-Security zu erhöhen, schließen Sie alle nicht von Ihrer Applikation benötigten Ports und Dienste in den Steuerungskomponenten (z. B. Port 6626 für WAGO-I/O-CHECK und Port 11740 für CO-DESYS V3).
- Öffnen Sie die Ports und Dienste nur für die Dauer der Inbetriebnahme bzw. Konfiguration.

Tabelle 61: WBM-Seite „Configuration of Network Services“ – Gruppe „I/O-CHECK“

Parameter	Bedeutung	
Service active	WAGO I/O-CHECK-Service aktivieren/deaktivieren;	
	<input type="checkbox"/>	Der WAGO I/O-CHECK-Service ist deaktiviert; Werkseinstellung
	<input checked="" type="checkbox"/>	Der WAGO I/O-CHECK-Service ist aktiviert.

### 3.5.3.8 SSH-Server

Tabelle 62: WBM-Seite „SSH Server Settings“ – Gruppe „SSH Server“

Parameter	Bedeutung	
Service active	SSH-Server-Dienst aktivieren/deaktivieren.	
	<input type="checkbox"/>	Der SSH-Server-Dienst ist deaktiviert.
	<input checked="" type="checkbox"/>	Der SSH-Server-Dienst ist aktiviert.
Port Number	Port-Nummer eingeben.	
Allow root login	Root-Zugriff sperren oder erlauben.	
Allow password login	Passwortabfrage aktivieren oder deaktivieren.	

### 3.5.3.9 Docker®

Tabelle 63: WBM-Seite „Docker Settings“ – Gruppe „Docker Status“

Parameter	Bedeutung	
Current State	Aktueller Status des Dienstes „Docker“	
	stopped	Der Dienst „Docker“ ist gestoppt.
	running	Der Dienst „Docker“ ist aktiv.
Service Enabled	Dienst „Docker“ aktivieren/deaktivieren;	
	<input type="checkbox"/>	Der Dienst „Docker“ ist deaktiviert.
	<input checked="" type="checkbox"/>	Der Dienst „Docker“ ist aktiviert.

## 3.6 Cloud-Connectivity

Mit der Cloud-Connectivity-Funktionalität und einer IEC-Bibliothek steht der Controller als Gateway für Anwendungen im Bereich Internet-of-Things (IoT) zur Verfügung. Damit kann der Controller die Daten aller angeschlossenen Geräte sammeln und über die eingebaute ETHERNET-Schnittstelle oder das Mobilfunkmodul auf das Internet zugreifen und die Daten in die Cloud senden.

Der zu nutzende Cloud-Dienst ist einstellbar, zur Verfügung stehen u. a. Microsoft Azure und Amazon Web Services.

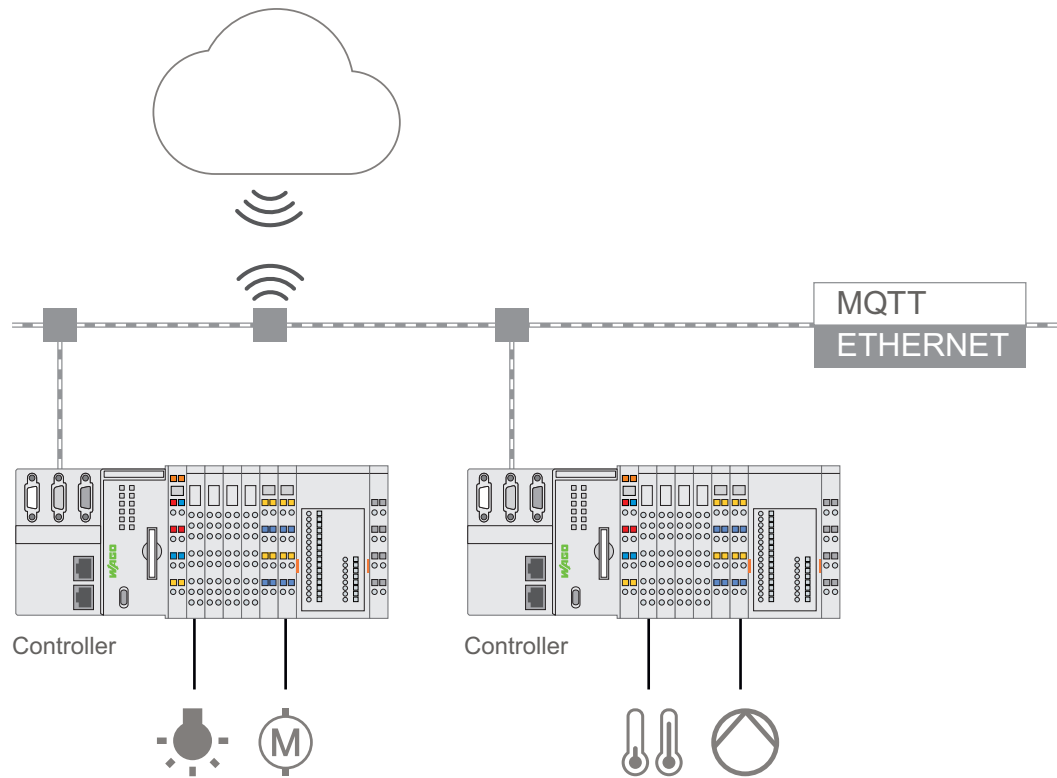


Abbildung 5: Anbindung der Controller an einen Cloud-Dienst (Beispiel)

Die Daten werden vom Controller zum Cloud-Dienst im JSON-Format übertragen. Die Verbindung kann per TLS verschlüsselt werden, siehe TLS-Verschlüsselung.

Einstellungen, die im Controller für die Nutzung der Cloud-Connectivity-Funktionalität vorgenommen werden müssen, finden Sie [Im Web-Based-Management \(WBM\) konfigurieren \[ > 89\]](#).

Die Konfiguration der Kommunikationsparameter erfolgt im z. B. im WBM.

Die Konfiguration der zwischen Cloud und Controller auszutauschenden Daten erfolgt aus der IEC-Applikation mit der entsprechenden CODESYS V3-Bibliothek.

Tabelle 64: Komponenten des Softwarepaketes Cloud-Connectivity

Komponente	Beschreibung
CODESYS V3: WagoAppCloud WagoAppSparkplug	IEC-Bibliotheken zum Erstellen der SPS-Applikation; Funktionsblöcke ermöglichen das Senden und Empfangen von Daten zwischen SPS und dem Cloud-Dienst. Die Variablen zur Datenübertragung sind definierbar.

**i Hinweis**

**Beachten Sie die zusätzlichen Dokumentationen!**

Sie finden eine detaillierte Beschreibung des Softwarepaketes Cloud-Connectivity mit einem Controller PFC100/200 und Informationen zur SPS-Programmierung im Anwendungshinweis A500920 im Downloadbereich unter [www.wago.com](http://www.wago.com).

## Hinweis

### Beachten Sie die erforderlichen Einstellungen zu Datenschutz und Sicherheit!

Bevor Sie die Cloud-Connectivity-Funktionalität nutzen, informieren Sie sich zum Thema Datenschutz und Sicherheit in dem entsprechenden Handbuch im Downloadbereich unter [www.wago.com](http://www.wago.com).

Tabelle 65: WBM-Seite „Overview“ – Gruppe „Connection <n>“

Parameter	Bedeutung
Operation	Status der Cloud-Connectivity-Applikation
Data from PLC Runtime	Anzahl der Data-Collections, die seitens der IEC-Applikation für die Übertragung zur Cloud registriert wurden
Cloud Connection	Status der Verbindung zum Cloud-Dienst
Heartbeat	Aktuell konfiguriertes Heartbeat-Intervall in Sekunden
Telemetry data transmission	Status der Datenübertragung
Cache fill level (QoS 1 and 2)	Füllstand des Speichers für ausgehende Nachrichten in Prozent

Tabelle 66: WBM-Seite „Configuration of Connection <n>“ – Gruppe „Configuration“

Parameter	Bedeutung
Enabled	Cloud-Connectivity-Funktionalität aktivieren/deaktivieren
Cloud platform	Cloud-Plattform
Hostname	Hostname oder IP-Adresse für die ausgewählte Cloud-Plattform
ID Scope	Endpunkt für den Azure Gerätebereitstellungsdienst (DPS)
Registration ID	Registrierungs-ID für den Azure Gerätebereitstellungsdienst (DPS)
Port number	Port-Nummer, zu dem eine Verbindung aufgebaut werden soll  Typische Werte: <ul style="list-style-type: none"> <li>• 8883 für verschlüsselte Verbindungen</li> <li>• 1883 für unverschlüsselte Verbindungen</li> </ul>
Device ID	Device-ID für die ausgewählte Cloud-Plattform
Client ID	Client-ID für die ausgewählte Cloud-Plattform
Authentication	Authentifizierungsmethode, z. B. „Shared Key Acces“, „X.509 Certificate“
Activation Key	Aktivierungsschlüssel für die ausgewählte Cloud-Plattform
Clean Session	Clean-Session bei der Verbindung zum Cloud-Dienst aktivieren  Clean-Session aktiv: Informationen und Nachrichten zu dieser Verbindung beim Cloud-Dienst nicht persistent gespeichert
TLS	Verwendung einer TLS-Verschlüsselung für die Verbindung zur Cloud-Plattform aktivieren/deaktivieren  Amazon Web Services (AWS) verwendet TLS
CA file	Pfad zu der im PEM-Format enkodierten Datei, die das für den Aufbau einer verschlüsselten Verbindung zu verwendende und vertrauenswürdige CA-Zertifikat enthält  Standardwert: CA-Zertifikat /etc/ssl/certs/ca-certificates.crt
User	Benutzername
Password	Passwort
Certification file	Pfad zu der im PEM-Format enkodierten Datei, die zur Authentisierung gegenüber dem Cloud-Dienst genutzt wird
Key file	Pfad zu der im PEM-Format enkodierten Datei, welche den privaten Schlüssel für die Authentisierung gegenüber dem Cloud-Dienst enthält

Parameter	Bedeutung
Use websockets	Verbindungsaufbau zur Cloud-Plattform mittels WebSocket-Protokoll über den Port 443 aktivieren/deaktivieren  Wenn deaktiviert: Verbindungsaufbau zur Cloud-Plattform mittels MQTT-Protokoll über den Port 8883
HTTP Proxy Host	Hostname oder IP-Adresse des Proxys
HTTP Proxy Port	Portnummer des Proxys
HTTP Proxy User	Name des Proxy-Benutzers
HTTP Proxy Password	Passwort des Proxy-Benutzers
Use compression	Datenkomprimierung mittels GZIP-Komprimierung aktivieren/deaktivieren
Data Protocol	Daten-Protokoll
Cache mode	Speicherort des Caches für die Datentelegramme  Auswahlfeld nur aktiv, wenn eine korrekt formatierte SD-Karte gesteckt ist Weitere Informationen: Anwendungshinweis A500920
Last Will	Last-Will-Nachricht aktivieren/deaktivieren  Nach Aktivierung erscheinen nachfolgend zusätzliche Eingabefelder
(Last Will) Topic	Topic, unter welchem die Last-Will-Nachricht versendet werden soll
(Last Will) Message	Nachricht, die als Last-Will-Nachricht versendet werden soll
(Last Will) QoS	„Quality of Service“ (QoS) der Last-Will-Nachricht
(Last Will) Retain	Letzte unter einem Topic gesendete Last-Will-Nachricht vom Broker als gespeicherte Nachricht (Retained Message) aktivieren/deaktivieren
Device info	Device-Info-Nachricht, welche den Cloud-Dienst über die grundlegende Konfiguration des Controllers informiert, aktivieren/deaktivieren Weitere Informationen: Anwendungshinweis A500920
Device status	Device-State-Nachrichten, welche den Cloud-Dienst über Änderungen des Betriebsartenschalters sowie der LEDs informiert, aktivieren/deaktivieren Weitere Informationen: Anwendungshinweis A500920
Standard commands	Integrierte Standardkommandos aktivieren/deaktivieren Weitere Informationen: Anwendungshinweis A500920 Wenn deaktiviert: Nur die im IEC-Programm definierten Kommandos unterstützt
Application property template	Eigenes Property für die einzelnen MQTT-Nachrichten zur Azure-Cloud erstellen  Parameter optional, d. h., wenn das Feld leer gelassen wird, wird dieses Property nicht mitgesendet  Platzhalter zur Erstellung: <ul style="list-style-type: none"> <li>▪ &lt;m&gt;: Nachrichtentype</li> <li>▪ &lt;p&gt;: Protokoll-Version</li> <li>▪ &lt;d&gt;: DeviceId</li> </ul> Beispiele: <ul style="list-style-type: none"> <li>▪ MyKey=HelloWorld_&lt;m&gt;</li> <li>▪ TestKey=&lt;m&gt;/&lt;p&gt;/&lt;d&gt;</li> <li>▪ DeviceId=&lt;d&gt;</li> </ul>

Tabelle 67: Anzeige der Auswahl- und Eingabefelder abhängig von der ausgewählten Cloud-Plattform

Auswahl- oder Eingabefeld	Cloud-Plattform					
	WAGO Cloud	Azure	MQTT Any-Cloud	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	

Auswahl- oder Eingabefeld	Cloud-Plattform					
	WAGO Cloud	Azure	MQTT Any-Cloud	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
X: Sichtbar und aktiv						
(X): Sichtbar, aber nicht aktiv						
X1: Sichtbar und aktiv, abhängig vom ausgewählten Datenprotokoll						
X2: Sichtbar und aktiv, abhängig von der ausgewählten Authentifizierung						
X3: Sichtbar und aktiv, wenn „Last Will“ eingeschaltet ist						
(X3): Sichtbar, aber nicht aktiv, wenn „Last Will“ eingeschaltet ist						
X4: Aktiv, wenn „Use websockets“ eingeschaltet ist						
X5: Sichtbar und aktiv, wenn „Use websockets“ eingeschaltet ist und wenn als „Proxy Type“ „HTTP“ eingestellt ist						

Tabelle 68: Auswahlmöglichkeit des Datenprotokolls abhängig von der ausgewählten Cloud-Plattform

Datenprotokoll	Cloud-Plattform					
	WAGO Cloud	Azure	MQTT Any-Cloud	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: Auswahl möglich						
(X): Fest eingestellt						

Tabelle 69: Anzeige der Auswahl- und Eingabefelder abhängig vom ausgewählten Datenprotokoll

Auswahl- oder Eingabefeld	Datenprotokoll			
	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: Sichtbar und aktiv				

Tabelle 70: Auswahlmöglichkeit des Cache-Modes abhängig vom ausgewählten Datenprotokoll

Cache-Mode	Datenprotokoll			
	WAGO Protocol	WAGO Protocol 1.5	Native MQTT	Sparkplug payload B
RAM	X	X	X	(X)
SD-Card	X1	X1	X1	
X: Auswahl möglich				
X1: Auswahl nur möglich, wenn "Compression" nicht eingeschaltet ist				
(X): Fest eingestellt				

Tabelle 71: Anzeige der Eingabefelder abhängig von der ausgewählten Authentifizierung

Auswahl- oder Eingabefeld	Authentifizierung	
	Shared Access Key	X.509 Certificate
Activation Key	X	
Certification file		X
Key file		X
X: Sichtbar und aktiv		

### 3.7 Feldbusfunktionen

#### 3.7.1 OPC UA

Tabelle 72: WBM-Seite „OPC UA Configuration“ – Gruppe „OPC UA Server Configuration“

Parameter	Bedeutung	
Enabled	OPC UA-Server aktivieren oder deaktivieren.	
	<input type="checkbox"/>	Der OPC UA-Server ist deaktiviert.
	<input checked="" type="checkbox"/>	Der OPC UA-Server ist aktiviert.
Log Level	Log-Levels auswählen; Die Auswahl des Log Levels beeinflusst die Reaktionszeit des Servers. Wählen Sie daher nur den minimal benötigten Level aus, z. B. „Debug“ nur für tiefgreifende Analysen. Folgende Werte sind einstellbar:	
	Error	Es werden nur Fehlermeldungen ausgegeben.
	Warning	Es werden Fehlermeldungen und Warnmeldungen ausgegeben.
	Info	Es werden Fehlermeldungen, Warnmeldungen und Statusmeldungen ausgegeben.
	Debug	Es werden Fehlermeldungen, Warnmeldungen, Statusmeldungen und zusätzlich Debug-Meldungen ausgegeben.
Ctrl Configuration Name	Konfigurationsnamen, den der Controller innerhalb des PLC Open Device Sets erhält, eingeben.	

Tabelle 73: WBM-Seite „OPC UA Configuration“ – Gruppe „OPC UA Server Security Settings“

Parameter	Bedeutung	
Anonymous Access	Anonymen Zugriff auf den Server sperren/zulassen.	
	<input type="checkbox"/>	Ein anonymer Zugriff ist nicht zulässig.
	<input checked="" type="checkbox"/>	Ein anonymer Zugriff ist zulässig; Dies setzt voraus, dass die Portauthentifizierung der Runtime ebenfalls deaktiviert ist/wird.
Allow Password On Plaintext	Übertragung des Passworts im lesbaren Format	
	<input type="checkbox"/>	
	<input checked="" type="checkbox"/>	
Security Modes	Security Mode des OPC UA Servers; Je nach Auswahl der Betriebsart stehen verschiedene OPC UA Endpoints zum Verbindungsaufbau zur Verfügung.	
	None	Lediglich der OPC UA Endpoint <b>None</b> wird aktiviert. Dieser ermöglicht eine ungesicherte Verbindung zum OPC UA Server.
	None + Sign + SignAndEncrypt	Die Endpoints <b>None</b> , <b>Sign</b> und <b>SignAndEncrypt</b> stehen zur Verfügung. <b>Sign</b> stellt einen Endpoint zur Verfügung, der über ein Passwort geschützt ist. <b>SignAndEncrypt</b> stellt einen Endpoint zur Verfügung, der neben einem Passwort auch eine Verschlüsselung ermöglicht.
	Sign + SignAndEncrypt	Die Endpoints <b>Sign</b> und <b>SignAndEncrypt</b> stehen zur Verfügung.
	SignAndEncrypt	Nur der Endpoint <b>SignAndEncrypt</b> steht zur Verfügung.

Parameter	Bedeutung
Security Policies	Auswahl der Security Policies; Hierüber wird die Verschlüsselungsstärke des OPC UA Servers eingestellt. Zur Auswahl stehen dabei: Aes128Sha256RsaOaep and better, Basic256Sha256 and better, Aes256Sha256RsaPss.

### 3.7.2 BACnet

BACnet ist eine lizenzpflichtige Erweiterung; die Lizenzierung kann mit Add-on-Licensing durchgeführt werden.

Für den produktiven, zeitlich unbegrenzten Einsatz von BACnet wird ein Lizenzschlüssel benötigt. Auch ohne Lizenzschlüssel ist BACnet zeitlich begrenzt in vollem Umfang nutzbar. Zu diesem Testzeitraum zählt nur die Zeit tatsächlicher Nutzung. Nach Ablauf des Testzeitraums ist ein Zugang ohne Lizenzschlüssel nicht mehr möglich.

#### Hinweis

##### Einschränkung der BACnet-Kommunikation

Die BACnet-Kommunikation ist nur über den Port X1 möglich, sowie über die Ports, die in der Netzwerkkonfiguration der Bridge 1 (br0) zugeordnet sind.

Weitere Informationen finden Sie im BACnet Protocol Implementation Conformance Statement (PICS) unter [www.wago.com](http://www.wago.com).

Tabelle 74: WBM-Seite „BACnet Status“ – Gruppe „BACnet Information“

Parameter	Bedeutung	
State	BACnet Feldbusstatus	
	<input type="checkbox"/>	Feldbus BACnet ist deaktiviert
	<input checked="" type="checkbox"/>	Feldbus BACnet ist aktiviert
Mode	BACnet Betriebsmodus	
	ip	Kommunikation über BACnet/IP
	sc	Kommunikation über BACnet/SC
Version	Installierte BACnet Version	
Status Info	BACnet Feldbusstatus	
Device-ID	Aktuelle Device-ID des Produkts	

Tabelle 75: WBM-Seite „BACnet Status“ – Gruppe „BACnet License“

Parameter	Bedeutung
Type	Anzeige der BACnet Lizenzen
User Objects	Anzeige der Anzahl der vorhandenen sowie der mit der Lizenz möglichen BACnet Objekte

Tabelle 76: WBM-Seite „BACnet Status“ – Gruppe „BACnet Data Link“

Parameter	Bedeutung
Connection Info	Anzeige des Verbindungsstatus

Tabelle 77: WBM-Seite „BACnet Configuration“ – Gruppe „PLC Runtime“

Parameter	Bedeutung
[Restart]	Neustart der Runtime ausführen

Tabelle 78: WBM-Seite „BACnet Configuration“ – Gruppe „BACnet Service“

Parameter	Bedeutung
Service active	Feldbus BACnet aktivieren/deaktivieren.
	<input type="checkbox"/> BACnet ist deaktiviert.
	<input checked="" type="checkbox"/> BACnet ist aktiviert.
Mode	Hier wählen Sie den BACnet Betriebsmodus aus.
	ip Kommunikation über BACnet/IP
	sc Kommunikation über BACnet/SC
Who-Is online interval time (sec)	Zeitlicher Abstand der Controller-Anfragen auf den Feldbus, welche weiteren Teilnehmer online sind (minimal: 60 sec).
Broadcast I-Am answer	Aktivieren/deaktivieren, dass die I-Am-Nachrichten des Gerätes an die BACnet Broadcast-Adresse gesendet werden.
	<input type="checkbox"/> I-Am-Nachrichten werden nicht an die BACnet Broadcast-Adresse gesendet.
	<input checked="" type="checkbox"/> I-Am-Nachrichten werden an die BACnet Broadcast-Adresse gesendet.

Tabelle 79: WBM-Seite „BACnet Configuration“ – Gruppe „BACnet Data“

Parameter	Bedeutung
Delete Persistence Data	Persistente BACnet-Daten werden beim nächsten Neustart gelöscht.
Reset all BACnet Data and Settings to Default	BACnet-spezifische Einstellungen und Daten werden beim nächsten Neustart auf Werkseinstellungen zurückgesetzt.
override.xml Chose file ...	Auswahl der gewünschten Datei auf dem PC
[Upload]	Übertragen der ausgewählten Datei vom PC zum Controller

Tabelle 80: WBM-Seite „BACnet Configuration“ – Gruppe „BACnet Log Level“

Parameter	Bedeutung
Error	Error-Logausgaben aktivieren/deaktivieren.
	<input type="checkbox"/> Error-Logeinträge werden nicht ausgegeben.
	<input checked="" type="checkbox"/> Error-Logeinträge werden ausgegeben.
Warning	Warning-Logausgaben aktivieren/deaktivieren.
	<input type="checkbox"/> Warning-Logeinträge werden nicht ausgegeben.
	<input checked="" type="checkbox"/> Warning-Logeinträge werden ausgegeben.
Info	Info-Logausgaben aktivieren/deaktivieren.
	<input type="checkbox"/> Info-Logeinträge werden nicht ausgegeben.

Parameter	Bedeutung	
	<input checked="" type="checkbox"/>	Info-Logeinträge werden ausgegeben.
Debug	Debug-Logausgaben aktivieren/deaktivieren.	
	<input type="checkbox"/>	Debug-Logeinträge werden nicht ausgegeben.
	<input checked="" type="checkbox"/>	Debug-Logeinträge werden ausgegeben.

Tabelle 81: WBM-Seite „BACnet Configuration“ – Gruppe „BACnet Network Capture“

Parameter	Bedeutung	
Enable	Aufzeichnung des Netzwerkverkehrs mit den entsprechenden BACnet Filtern aktivieren/deaktivieren.	
	<input type="checkbox"/>	Netzwerkverkehr wird nicht aufgezeichnet.
	<input checked="" type="checkbox"/>	Netzwerkverkehr wird aufgezeichnet.
Log pre-master secrets	Speicherung der Secrets für die Entschlüsselung des BACnet/SC Netzwerkverkehrs aktivieren/deaktivieren.	
	<input type="checkbox"/>	Secrets werden nicht gespeichert.
	<input checked="" type="checkbox"/>	Secrets werden gespeichert.
BACnet Network Capture Archive [Download]	Über die Schaltfläche [Download] können Sie den aufgezeichneten Netzwerkverkehr incl. der Secrets, falls die Option aktiviert ist, vom Gerät herunterladen.	

Tabelle 82: WBM-Seite „BACnet Data Link“ – Gruppe „BACnet Restart“

Parameter	Bedeutung
[Restart]	Neustart des BACnet Dienstes

Tabelle 83: WBM-Seite „BACnet Data Link“ – Gruppe „BACnet/IP“

Parameter	Bedeutung
Port Number	Eingabe des Ports für die BACnet/IP Kommunikation

Tabelle 84: WBM-Seite „BACnet Data Link“ – Gruppe „BACnet/SC“

Parameter	Bedeutung	
Mode	Auswahl der BACnet/SC Betriebsart	
	regular	Das Gerät wird als BACnet/SC Node betrieben.
	primary	Das Gerät wird als BACnet/SC Primary HUB betrieben.
	failover	Das Gerät wird als BACnet/SC Failover HUB betrieben.
Port Number	Eingabe des Ports für die BACnet/SC Kommunikation	
Primary Hub URI	Eingabe des URI für den Primary HUB; wss://<IP-Adresse>:<Port des HUBs> bzw. wss://<Domainname>:<Port des HUBs> (z. B. wss://192.168.178.19:47808 bzw. wss://PFC200V3-XXXXXX.localdomain.lan:47808)	

Parameter	Bedeutung
Failover Hub URI	Eingabe des URI für den Failover HUB; wss://<IP-Adresse>:<Port des HUBs> bzw. wss://<Domainname>:<Port des HUBs> (z. B. wss://192.168.178.19:47808 bzw. wss://PFC200V3-XXXXXX.localdomain.lan:47808)
Allow self signed Certificates	Aktivieren/deaktivieren, ob die Kommunikation über selbstsignierte Zertifikate aufgebaut werden darf.
Allow expired Certificates	Aktivieren/deaktivieren, ob die Kommunikation über abgelaufene Zertifikate aufgebaut werden darf.
Allow any Certificates	Aktivieren/deaktivieren, ob die Kommunikation über beliebige Zertifikate aufgebaut werden darf.

Tabelle 85: WBM-Seite „BACnet Data Link“ – Gruppe „BACnet/SC Certificate Authority (CA)“

Parameter	Bedeutung
Chose file ...	Auswahl des CA-Zertifikats auf dem Computer für die Übertragung auf das Gerät
<b>[Upload]</b>	Übertragung des ausgewählten CA-Zertifikats auf das Gerät; Nach dem Neustart wird dieses Zertifikat als CA-Zertifikat für die BACnet/SC Kommunikation verwendet.

Tabelle 86: WBM-Seite „BACnet Data Link“ – Gruppe „BACnet/SC Certificate“

Parameter	Bedeutung
Chose file ...	Auswahl des Gerätezertifikats auf dem Computer für die Übertragung zum Gerät
<b>[Upload]</b>	Übertragung des ausgewählten Gerätezertifikats auf das Gerät; Nach dem Neustart wird dieses Zertifikat für die BACnet/SC Kommunikation verwendet.

Tabelle 87: WBM-Seite „BACnet Configuration“ – Gruppe „BACnet/SC Certificate Signing Request (CSR)“

Parameter	Bedeutung
Country	Eingabe des Landes für den CSR bzw. für das Gerätezertifikat (zwei Buchstaben)
State	Eingabe des Staates für den CSR bzw. für das Gerätezertifikat
Locality	Eingabe des Ortes für den CSR bzw. für das Gerätezertifikat
Organization	Eingabe der Firma bzw. der Organisation für den CSR bzw. für das Gerätezertifikat
Organizational Unit	Eingabe der Abteilung für den CSR bzw. für das Gerätezertifikat
Common Name	Eingabe des Gerätenamens für den CSR bzw. für das Gerätezertifikat
<b>[Generate]</b>	Erstellung eines CSR sowie eines neuen privaten Schlüssels auf dem Gerät
<b>[Download]</b>	CSR vom Gerät herunterladen

Tabelle 88: WBM-Seite „BACnet Data Link“ – Gruppe „BACnet/SC Default Certificates“

Parameter	Bedeutung
<b>[Generate]</b>	Erstellung eines neuen Zertifikates

Tabelle 89: WBM-Seite „BACnet Storage Location“ – Gruppe „BACnet Persistence“

Parameter	Bedeutung	
Storage Location	Speicherort für die Persistenzdaten auswählen; Die Auswahl ist nur möglich, wenn beide Speicher vorhanden sind.	
	Internal Flash	Die Daten werden im internen Speicher des Controllers gespeichert.
	SD-Card	Die Daten werden auf der Speicherkarte gespeichert. Wenn „SD-Card“ ausgewählt ist, aber die Speicherkarte nicht mehr gesteckt ist, dann ist diese Option nicht mehr aktiv und nur noch „Internal Flash“ auswählbar.

Tabelle 90: WBM-Seite „BACnet Storage Location“ – Gruppe „BACnet Trendlog“

Parameter	Bedeutung	
Storage Location	Speicherort für die Trendlogdaten auswählen; Die Auswahl ist nur möglich, wenn beide Speicher vorhanden sind.	
	Internal Flash	Die Daten werden im internen Speicher des Controllers gespeichert.
	SD-Card	Die Daten werden auf der Speicherkarte gespeichert. Wenn „SD-Card“ ausgewählt ist, aber die Speicherkarte nicht mehr gesteckt ist, dann ist diese Option nicht mehr aktiv und nur noch „Internal Flash“ auswählbar.

Tabelle 91: WBM-Seite „BACnet Storage Location“ – Gruppe „BACnet Eventlog“

Parameter	Bedeutung	
Storage Location	Speicherort für die Eventlogdaten auswählen; Die Auswahl ist nur möglich, wenn beide Speicher vorhanden sind.	
	Internal Flash	Die Daten werden im internen Speicher des Controllers gespeichert.
	SD-Card	Die Daten werden auf der Speicherkarte gespeichert. Wenn „SD-Card“ ausgewählt ist, aber die Speicherkarte nicht mehr gesteckt ist, dann ist diese Option nicht mehr aktiv und nur noch „Internal Flash“ auswählbar.

### 3.7.3 CANopen-Master und -Slave

Entsprechend der IEC 61131-3-Programmierung erfolgt die Bearbeitung der Prozessdaten vor Ort im Controller. Die daraus erzeugten Ergebnisse können direkt an die Aktoren ausgegeben oder über den Bus übertragen werden.

Der Prozessdatenaustausch findet mit PDOs und SDOs statt. Um Prozessdaten über den CANopen-Feldbus zu versenden, unterstützt der Controller 512 TXPDOs und 512 RX-PDOs sowie 128 SDOs.

Im lokalen Prozessabbild ist ein Bereich von je 4096 Byte als Eingangs- und Ausgangsbereich für den Datenaustausch über die CANopen-Schnittstelle vorgesehen. Ein direkter Zugriff auf die I/O-Module über den Feldbus ist nicht vorgesehen.

Die Einträge im Prozessabbild können nach Bedarf auf die RX PDOs und TX PDOs gemappt werden. Der gesamte Eingangs- und Ausgangsbereich kann mit den SDOs gelesen und geschrieben werden.

Die CANopen-Kommunikation läuft nach der Initialisierung unabhängig von der IEC Applikation. Bei der Verwendung als CANopen-Slave ist das Ändern der Baudrate und der Busadresse gemäß dem CANopen-LSS-Protokoll möglich.

### 3.7.3.1 Objektverzeichnis

Alle CANopen-Kommunikations- und Prozessdatenobjekte werden im Objektverzeichnis zusammengefasst.

Die folgende Tabelle gibt einen groben Überblick über die Festlegung in der CANopen-Definition:

Tabelle 92: Übersicht über die Adressen im Objektverzeichnis

Indxbereich	Verwendung
0000	Nicht genutzt
0001-009F	Datentypen
00A0-0FFF	Reserviert (Adressen genutzt für andere Dienste)
1000-1FFF	Kommunikationsprofil
2000-5FFF	Herstellerspezifischer Bereich
6000-9FFF	Bis zu 8 standardisierte Geräteprofile
A000-AFFF	Prozessabbilder von IEC61131-Geräten
B000-BFFF	Prozessabbilder von CANopen-Gateways nach CiA 302-7
C000-FFFF	Reserviert

Die am PFC verfügbaren und relevanten Objekte werden nachfolgend beschrieben.

### 3.7.3.2 Kommunikationsprofil

#### 0x1000 Device type

Der Stack meldet sich auf dem Bus als DS-405 (IEC61131-3 programmable device) Device, unabhängig ob er als Master oder als Slave konfiguriert ist. Da kein direkter Zugriff über den Bus auf die I/O-Module zugelassen wird, sind die Bits für die Information über Ein- und Ausgänge 0.

Eintrag 0x000195 = DS 405 für Master und Slave

#### 0x1001 Error Register

Dieser Eintrag enthält eine 8 Bit-Information über den Fehlerzustand. Derzeit werden die Bits 4 für Kommunikation und Bit 5 für Geräteprofil spezifisch genutzt. Das Bit 0 wird bei jedem Fehler gesetzt.

#### 0x1003 Pre-defined Error Field

Dieser Eintrag enthält die Liste der aufgelaufenen Fehler, die im Error Register 0x1001 signalisiert wurden. Subindex 0 enthält die Anzahl der Einträge. Tritt ein neuer Fehler auf, so wird dieser in Sub-Index 1 eingefügt und alle schon existierenden um einen Sub-Index nach unten verschoben. Es werden max. 20 Fehlereinträge unterstützt. Treten mehr als 20 Fehler auf, so wird jeweils der Fehler auf Sub-Index 20 überschrieben. Durch Schreiben einer „0“ in den Sub-Index 0, wird der komplette Fehlerspeicher gelöscht.

Standardwerte: 0 in allen Einträgen

**0x1005 COB IB Sync**

Das Objekt legt die COB-ID für die Synchronisationsnachricht fest.

Standardwert: 0x80

**0x1006 Communication Cycle Period**

Die Periodenlänge des Synchronisationszyklus in  $\mu\text{s}$  oder 0 für keine zyklische Synchronisation. Die Auflösung intern beträgt 1ms. Ist der Wert 0 wird keine SYNC-Überwachung durchgeführt.

Standardwert: 0

**0x1008 Manufacturer Device Name**

Das Objekt gibt den Gerätenamen an.

Eintrag: Bestellnummer des PFC200, z. B. „750-8216“

**0x1009 Manufacturer Hardware Version**

Eintrag: „V 1.0“ oder höher

**0x100A Manufacturer Software Version**

Eintrag: „04.02.05(00)“ oder höher

**0x100C Node Guarding Time**

Das Objekt gibt die Guarding Time in Millisekunden an. Ein NMT-Master fragt zyklisch den NMT Slave nach seinem Zustand ab. Die Zeit zwischen zwei Anfragen ist die Guard Time.

Standardwert: 0 (Node Guarding deaktiviert)

**0x100D Life Time Factor**

Der Life Time Factor ist ein Teil des Node-Guarding Protocols. Der NMT-Slave überprüft, ob er innerhalb der Node Life Time (Guardtime multipliziert mit dem Life Time Factor) abgefragt wurde. War dies nicht der Fall, so muss der Slave davon ausgehen, dass sich der NMT-Master nicht mehr im normalen Betrieb befindet und löst dann ein Life Guarding Event aus.

Standardwert: 0 (Node Guarding aus)

**0x1012h COB-ID Time Stamp Object**

Das Time-Stamp Objekt ermöglicht die Synchronisation der Uhren aller Geräte am Bus. Die ID für dieses Objekt wird hier angegeben. Das Synchronisations-Signal wird von der Runtime nicht selbst ausgewertet, kann aber mit Bibliotheksfunktionen genutzt werden.

Standardwert: 0x100 (Time Stamp Consumer)

**0x1014h Emergency COB-ID**

Bei Fehlern des CANopen Gerätes wird eine Emergency Message versandt. Die ID für dieses Objekt wird hier angegeben (beim Master Read-Only).

Standardwert: 0x80 + Geräte ID

**0x1015h Emergency Inhibit time**

Dieses Objekt gibt die minimale Zeit an, die vergehen muss, bevor eine weitere Emergency Message gesendet wird. Ein Eintrag gleich Null deaktiviert das verzögerte Senden. Eine Zeiteinheit beträgt 100µs.

Standardwert: 0

**0x1016h Consumer heartbeat time**

Mit diesem Eintrag ist die Überwachung von anderen Geräten auf dem Bus möglich. Es wird geprüft ob jedes in diesem Objekt definierte Modul innerhalb der eingestellten Zeit ein Heartbeat erzeugt hat. Wurde die eingestellte Zeit überschritten, wird ein Heartbeat-Event ausgelöst. Die Heartbeat-Time ist in Millisekunden eingetragen. Ist die Zeit 0, so ist die Überwachung deaktiviert. Im Index 0 wird die Anzahl der zu überwachenden Geräte eingetragen, in den anderen Einträgen die Heartbeatzeit in ms in den untersten 16 Bit und die ID des Bus-Gerätes in den 8 Bit darüber.

Standardwerte:

Index 0: 0 (z. Zt. noch 127 = Anzahl der möglichen Einträge)

Alle anderen Einträge 0 (Diese Funktion wird vom CAN-Master in der Firmware 1.0 noch nicht unterstützt.)

**0x1017h Producer heartbeat time**

Das Objekt legt die Zeit in Millisekunden zwischen zwei gesendeten Heartbeat- Nachrichten fest. Ist die Zeit 0 wird kein Heartbeat gesendet.

Standardwert: 0

**0x1018h Identity**

Das Objekt spezifiziert das verwendete Gerät. Die Hersteller-ID beinhaltet eine für jeden Hersteller eindeutige Zahl. WAGO wurde die ID 33 zugewiesen.

Der Product Code enthält die Gerätekennung.

Die Rev.-Nr. beinhaltet ein bestimmtes CANopen Verhalten. Dabei enthält die Major Rev. Nr. die CANopen Funktionalität. Wird die Funktionalität verändert, wird die Major Rev. Nr. erhöht. Anhand der Minor Rev. Nr. kann man verschiedene Versionen mit dem gleichen CANopen Verhalten unterscheiden.

Die Nummer ist unabhängig von der Firmware Revision. Bei der Verwendung als CANopen Slave mit CODESYS 3.5 können Vendor ID, Product Code und Revision Number in der Slave-Konfiguration frei festgelegt werden.

Subindex 0	Anzahl Einträge:	4
Subindex 1	Vendor ID:	33
Subindex 2	Product_code:	z. B. 8216 für 750-8216
Subindex 3	Revision_number:	0x00010003 oder höher
Subindex 4	Serial_number	entspricht den letzten 4 Byte der MAC-Adresse.

**0x1200 Server SDO Parameter Channels**

Hier sind die Kommunikationsparameter für einen SDO-Transfer als Server eingetragen. Es wird 1 Server SDO Kanal unterstützt.

**0x1280 ... 0x128E Client SDO Parameter Channels**

Hier sind die Kommunikationsparameter für einen SDO-Transfer als Client eingetragen. Es werden 16 Client SDO Kanäle unterstützt.

**0x1029h Error behavior**

Dieses Objekt legt fest, wie sich der der Slave bei einem Fehler verhält.

Subindex 0	Anzahl Einträge:	1	
Subindex 1	Communication Error:	1	Keine Änderung (Standard)
		0	Wechsel von Operational auf Preoperational
		2	Wechsel auf Stopp

**0x1F51 Programm Control**

Bei diesem Objekt kann der Zustand der SPS ausgelesen werden. Schreiben ist nicht zulässig.

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

**3.7.3.2.1 Masterkonfiguration**

Diese Objekte stehen busseitig nur zur Verfügung, wenn der Master konfiguriert ist.

**0x102A NMT Inhibit Time**

Dieses Objekt gibt die min. Zeit an, die vergehen muss, bevor ein weiteres NMT Telegramm gesendet wird. Ein Eintrag gleich Null deaktiviert das verzögerte Senden. Eine Zeiteinheit beträgt 100 µs.

Standardwert: 0

**0x1F80 NMT Startup**

Dieses Objekt enthält die Konfigurations Bits für den Status des Masters. Wird das automatische Starten deaktiviert, so kann durch das Schreiben von 0x1F auf dieses Objekt der Master gestartet werden.

**0x1F81 ... 0x1F8A Slave Konfiguration**

In diesen Listen sind die konfigurierten Slaves eingetragen. Alle Einträge werden beim Start des Masters geprüft bzw. an die Slaves übertragen.

**0x1F81 NMT Slave Assignment**

Subindex 0:	128 = Anzahl der möglichen Einträge
Subindex 1 ... 128:	Bit 0: Slave vorhanden
	Bit 2: Slave ist Pflicht beim Start
	Bit 3: Slave-Reset wird beim Start durchgeführt.
	Bit 8 ... 15: Guard Retry Factor
	Bit 16 ... 31: Guard Time
Subindex 128:	Gesamtes Netzwerk (Write-Only)

**0x1F82 Request NMT**

Subindex 0: 127 = Anzahl der möglichen Einträge

Subindex = Master Node ID NMT State des Masters

**0x1F84 Device type identification**

Subindex 0: 127 = Anzahl der möglichen Einträge

Subindex 1 ... 127: Device Type des Slaves

**0x1F85 Vendor identification**

Subindex 0: 127 = Anzahl der möglichen Einträge

Subindex 1 ... 127: Vendor Identification des Slaves (Standardmäßig nicht genutzt)

**0x1F86 Product code**

Subindex 0: 127 = Anzahl der möglichen Einträge

Subindex 1 ... 127: Product Code des Slaves (Standardmäßig nicht genutzt)

**0x1F87 Revision number**

Subindex 0: 127 = Anzahl der möglichen Einträge

Subindex 1 ... 127: Revision Number des Slaves (Standardmäßig nicht genutzt)

**0x1F88 Serial number**

Subindex 0: 127 = Anzahl der möglichen Einträge

Subindex 1 ... 127: Serial Number des Slaves (Standardmäßig nicht genutzt)

**0x1F89 Boot Time**

Zeit in ms zwischen Start der Slaves und Betriebsbereitschaft aller Slaves

Standardwert: 0 = deaktiviert

**0x1F8A Restore configuration**

Subindex 0: 127 = Anzahl der möglichen Einträge

Subindex 1 ... 127: Bit 0 = 1 Sende Restore Configuration beim Start zum Slave

**3.7.3.3 Datenaustausch**

Der Austausch der Prozessdaten findet bei dem CANopen Feldbus-Controller über die Kommunikationsobjekte statt.

Jedes Objekt besteht aus einem CAN-Telegramm, das maximal 8 Byte Nutzdaten und eine im Netzwerk eindeutige COB-ID (Communication Object Identifier) enthält.

Mittels dieser Kommunikationsobjekte erfolgt die Übertragung von Daten, das Auslösen von Events, das Signalisieren von Fehlerzuständen, usw.

Die für die Kommunikationsobjekte notwendigen Parameter, sowie Parameter und Daten des CANopen Teilnehmers sind in einem Objektverzeichnis abgelegt.

### 3.7.3.3.1 Kommunikationsobjekte des Controllers

Der Controller unterstützt folgende Kommunikationsobjekte:

- 512 Tx-PDOs für den Prozessdatenaustausch von Eingangsdaten des Feldbusknotens,
- 512 Rx-PDOs für den Prozessdatenaustausch von Ausgangsdaten des Feldbusknotens,
- Synchronisationsobjekte (SYNC) zur Netzwerksynchronisation,
- Emergency Objekte (EMCY)
- Netzwerkmanagement-Objekte
  - Module Control Protocols,
  - Error Control Protocols, kte
  - Bootup Protocol.

### 3.7.3.3.2 Feldbusspezifische Adressierung

Nach Konfiguration der CAN-Schnittstelle als Master oder als Slave werden die CODESYS Variablen für den CAN-Bus in ein Objektverzeichnis gemappt (Initialisierung). Ein CANopen Feldbus-Gerät verwendet die 16Bit-Indizes und 8Bit-Sub-Indizes des Objektverzeichnisses, um die Daten über PDOs oder SDOs zu adressieren und darauf zuzugreifen. Die Lage der Daten im Prozessabbild hat deshalb für den CANopen-Nutzer auf der Feldbusseite keine unmittelbare Bedeutung.

Der Eintrag der Variablen in das Objektverzeichnis erfolgt getrennt nach Datentyp (Integer8, Unsigned8, Boolean, Integer16, usw.) und Ein- und Ausgang. Der Zugriff über PDOs kann lesend oder schreibend sein.

Da CANopen die Daten nicht bitweise überträgt, werden die Variablendaten vom Datentyp Boolean zu Bytes zusammengefasst und dem entsprechenden Index zugeordnet, Eingangsvariablendaten vom Typ Boolean dem Index 0xA080, Ausgangsvariablendaten vom Typ Boolean dem Index 0xA500.

Die Zuordnung der Variablendaten, die eine Datenbreite von 1 Byte oder mehr haben, erfolgt zu den jeweiligen Indizes analog.

#### **i Hinweis**

#### **Datenrichtung beachten!**

Die IEC 61131-3 Eingangs- und Ausgangsvariablen sind definiert aus Sicht des CAN-Feldbusses,

d. h. :

IEC 61131-3 Eingangsvariablen sind PFC-Ausgangsvariablen und

IEC 61131-3 Ausgangsvariablen sind PFC-Eingangsvariablen.

Eine Übersicht über die Indizes der „IEC 61131-3“-Variablen zeigt die Tabelle.

Tabelle 93: Indizierung der „IEC 61131-3“-Variablendaten im Objektverzeichnis

Datentyp	„IEC 61131-3“-Ausgangsvariablen	„IEC 61131-3“-Eingangsvariablen
	Index	
Integer8	0xA000	0xA480
Unsigned8	0xA040	0xA4C0
Boolean	0xA080	0xA500
Integer16	0xA0C0	0xA540
Unsigned16	0xA100	0xA580
Integer24	0xA140	0xA5C0

Datentyp	„IEC 61131-3“-Ausgangsvariablen	„IEC 61131-3“-Eingangsvariablen
	Index	
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

Durch die zugehörigen Indizes für Datentypen mit der Datenbreite 1 Byte (Integer8, Unsigned8 und Boolean) kann vom Feldbus aus byteweise auf die Daten im Speicher des Controllers lesend zugegriffen werden.

Mit dem Sub-Index wird jeweils ein bestimmtes Byte ausgewählt.

Mit Verwendung der Indizes für größere Datenblöcke ist dagegen der Zugriff auf mehrere Bytes gleichzeitig möglich.

Mit dem Index für Integer16 (0xA0C0) oder für Unsigned16 (0xA100) kann z. B. wortweise auf die beschriebenen PFC-Ausgangsvariablen zugegriffen werden, mit dem Index 0xA140 für Integer24 auf 3 Byte usw.

**Beispiel:**

Auf die ersten drei Byte der PFC-Ausgangsdaten erfolgt ein Zugriff vom Feldbus aus mit dem Datentyp Integer, bzw. mit Unsigned:

Tabelle 94: Feldbuszugriff auf die PFC-Ausgangsdaten

Zugriff	PFC-Ausgangsdaten	Lesen mit dem Index (Integer / Unsigned)	Sub-Index
Byteweise (mit Integer8 / Unsigned8)	Byte 6000	(0xA000 / 0xA040)	1
	Byte 6001	(0xA000 / 0xA040)	2
	Byte 6002	(0xA000 / 0xA040)	3
Wortweise (mit Integer16 / Unsigned16)	Wort 3000 (Byte 6000/6001)	(0xA0C0 / 0xA100)	1
	Wort 3001 (Byte 6002/6003)	(0xA0C0 / 0xA100)	2
3 Byte (mit Integer24 / Unsigned24)	Bytes 6000 ... 6002	(0xA140 / 0xA180)	1

Die nachfolgenden Tabellen zeigen eine Übersicht über die Adressierung der Daten mit verschiedenen Datenbreiten.

Dazu ist dem Speicherplatz für die Feldbusvariablen (Byte 6000 bis Byte 9999) die jeweilige Indizierung in Abhängigkeit zur Datenbreite zugeordnet.

Die in den Tabellen angedeutete Indizierung wird bis zu dem jeweiligen maximalen Index und Sub-Index fortgeführt.

Hinweis t.b.d. (wie oben ???)

Abbildung t.b.d.

### 3.7.3.3.3 Beispiele für die Definition von PFC-Feldbusvariablen

In den folgenden Beispielen sind einige Definitionen für PFC-Variablen mit verschiedenen Datentypen den dazugehörigen Objektverzeichniseinträgen gegenübergestellt.

#### 3.7.3.3.3.1 CODESYS Zugriff auf PFC-Variablen

Tabelle 95: Beispiele für den CODESYS Zugriff auf PFC-Variablen

Datentyp der PFC-Variablen	PFC-Eingangsvariablen		PFC-Ausgangsvariablen	
	Definition nach IEC 61131-3	Index/Sub-Index	Definition nach 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

#### 3.7.3.3.3.2 Maximale Indizes

Die maximalen Indizes und Sub-Indizes ergeben sich aus der Speichergröße des Feldbus-Controllers mit 4096 Byte und der jeweiligen Datenbreite der Datentypen.

Eine Übersicht über die maximalen Indizes und Sub-Indizes der IEC 61131-3 Variablen zeigt die Tabelle.

Tabelle 96: Maximale Indizes und Sub-Indizes für „IEC 61131-3“-Variablen

Datentyp	„IEC 61131-3“-Ausgangsvariablen		„IEC 61131-3“-Eingangsvariablen	
	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

Datentyp	„IEC 61131-3“-Ausgangsvariablen		„IEC 61131-3“-Eingangsvariablen	
	Max. Index	Max. Sub-Index	Max. Index	Max. Sub-Index
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

**Beispiel:**

514 Bytes Ausgangsvariablen werden wortweise mit dem Datentyp Unsigned16 adressiert.

Die Adressierung der 257 Datenworte erfolgt dann mit:

- Index 0xA580, Sub-Index 1 bis 255 und
- Index 0xA581, Sub-Index 1 und 2.

Tabelle 97: Beispiel für „IEC 61131-3“-Ausgangsvariablen

Index	Sub-Index	Inhalt	Beschreibung
0xA580	1	D1 *)	1. Ausgangsvariablenblock
	2	D2 *)	2. Ausgangsvariablenblock
	...	...	...
	255	D255 *)	255. Ausgangsvariablenblock
0xA581	1	D256 *)	256. Ausgangsvariablenblock
	2	D257 *)	257. Ausgangsvariablenblock

\*) D1 = Datenwort Ausgangsvariable 1, D255 = Datenwort Ausgangsvariable 255, etc.

### 3.7.3.3.4 Verwendung des CANopen Slave (Device) unter CODESYS V3

Der CODESYS 3.5-Slave-Konfigurator verwendet andere Objekt Adressen für die Prozessdaten als in der CANopen Norm CiA 405 für IEC 61131 Geräte definiert sind. Beim Betrieb als CODESYS V3-Slave werden daher die CODESYS V3-Objektnummern verwendet:

0x3000 .. 0x31FF	Prozessdaten Empfang (Master => Slave)
0x3800 .. 0x39FF	Prozessdaten Senden (Slave => Master)
0x5000 .. 0x507F	SDO Lese/Schreibzugriff
0x5800 .. 0x587F	SDO Lesezugriff

Die nähere Beschreibung der Verwendung der CANopen-Schnittstelle ist im CODESYS V3-Online-Handbuch beschrieben. Die WAGO spezifischen Funktionen sind über die Bibliotheken WagoAppCanOpen und WagoAppCanLayer2 nutzbar.

### 3.7.3.3.5 Verwendung als CAN Layer 2 Gerät

Alternativ zur CANopen-Master- oder Slave-Funktion ist zusätzlich ein reiner Layer2-Stack auf dem Controller verfügbar. Dieser kann verwendet werden, wenn keine CANopen-Funktionen benötigt werden. Er bietet einen höheren Datendurchsatz bei einer geringeren CPU-Lastung.

Es können 127 Empfangsfilter mit einem Gesamtpuffer von 127 Telegrammen gesetzt werden oder ungefiltert mit einem Empfangspuffer von 255 Telegrammen gearbeitet werden.

Zur Nutzung mit CODESYS V3 wird das WAGO CanLayer2-Device am CAN ausgewählt. Die Funktionalität wird über die WagoAppCanLayer2-Bibliothek genutzt.

## 3.8 Speicherfunktionen

### 3.8.1 Datensicherung

Zur Sicherung und Wiederherstellung besitzt der Controller die Backup- und die Restore-Funktion.

Im WBM können die notwendigen Einstellungen im Register „Configuration“ auf den Seiten „Package Server“ > „Firmware Backup“ bzw. „Firmware Restore“ vorgenommen und die Funktionen ausgeführt werden.

Einstellbar ist das Speichermedium (Interner Speicher oder Speicherkarte) und ggf. der Speicherort im Netzwerk.

Weiterhin können die zu sichernden und wiederherzustellenden Daten ausgewählt werden:

- Das CODESYS Projekt („PLC-Runtime-Projekt“, Bootprojekt, CODESYS Einstellungen)
- Die Geräteeinstellungen („Settings“)
- Das Controllerbetriebssystem und das Root-Dateisystem („System“)
- Alle vorherigen („All“), nur sichtbar, wenn nicht im Netzwerk gespeichert wird

#### Hinweis

##### **Firmwareversion beachten!**

Das Wiederherstellen des Betriebssystems (Auswahl „System“) ist nur zulässig und möglich, wenn die Firmwareversionen zum Sicherungs- und Wiederherstellungszeitpunkt gleich sind. Verzichten Sie ggf. auf die Wiederherstellung des Betriebssystems oder gleichen Sie vorher die Firmwareversion an die Firmwareversion zum Sicherungszeitpunkt an.

#### 3.8.1.1 Backup-Funktion

Mit der Backup-Funktion können während des Betriebes die Daten des internen Speichers und Geräteeinstellungen auf der Speicherkarte gespeichert werden.

Als Zielmedium kann das Netzwerk oder, wenn gesteckt, die Speicherkarte ausgewählt werden.

Die Dateien des internen Laufwerks werden auf dem Zielmedium im Verzeichnis media/sd/copy und den entsprechenden Unterverzeichnissen abgelegt. Informationen, die nicht als Dateien in dem Controller vorliegen, werden im XML-Format im Verzeichnis media/sd/settings abgelegt.

Wenn die Speicherkarte als Zielmedium ausgewählt ist, blinkt die LED des Speicherkartensteckplatzes während des Speichervorgangs gelb/orange.

Die Geräteeinstellungen und Dateien des internen Laufwerks sind anschließend auf dem Zielmedium gesichert.

Der Controller verfügt über eine automatische Updatefunktion. Wird diese Funktion vor dem Sichern der Daten auf eine Speicherkarte aktiviert, und ein Controller von dieser Speicherkarte gebootet, dann wird automatisch eine Wiederherstellung dieser Daten auf dem internen Speicher des Controllers durchgeführt.

**i Hinweis****Nur ein Package zum Netzwerk kopierbar!**

Wenn Sie „Network“ als Speicherziel eingestellt haben, ist je Speichervorgang nur ein Package auswählbar.

**i Hinweis****Kein Back-up von Speicherkarte!**

Von der Speicherkarte aus ist ein Back-up auf den internen Flash-Speicher nicht möglich.

**i Hinweis****Back-up-Zeit berücksichtigen**

Das Erzeugen der Back-up-Dateien kann einige Minuten dauern. Stoppen Sie vor dem Back-up-Vorgang das CODESYS Programm, um diese Zeit weiter zu verkürzen.

Die Backup-Funktion kann über die WBM-Seite „Firmware Backup“ im Register „Configuration“, Auswahl „Package Server“ > „Firmware Backup“ aufgerufen werden.

Tabelle 98: WBM-Seite „Firmware Backup“ – Gruppe „Firmware Backup“

Parameter	Bedeutung	
Boot Device	Speichermedium, von dem das Gerät gebootet wurde	
Destination	Memory Card	Die Daten werden auf die Speicherkarte geschrieben. Diese Auswahl ist nur sichtbar, wenn eine Speicherkarte gesteckt ist und nicht von dieser gebootet wurde.
	USB-Stick	Die Daten werden auf den USB-Stick geschrieben. Diese Auswahl ist nur bei Produkten mit USB-Anschluss vorhanden. Die Auswahl ist nur aktiv, wenn ein USB-Stick gesteckt ist und nicht von diesem gebootet wurde.
	Network	Die Daten werden im File-System gespeichert und anschließend auf dem PC als Download zur Verfügung gestellt.
PLC Runtime Project	<input type="checkbox"/>	SPS-Laufzeit-Projekt wird nicht gesichert.
	<input checked="" type="checkbox"/>	SPS-Laufzeit-Projekt wird gesichert.
Settings	<input type="checkbox"/>	Geräteinstellungen werden nicht gesichert.
	<input checked="" type="checkbox"/>	Geräteinstellungen werden gesichert.
System	<input type="checkbox"/>	Betriebssystem des Geräts und Root-Dateisystem werden nicht gesichert.
	<input checked="" type="checkbox"/>	Betriebssystem des Geräts und Root-Dateisystem werden gesichert.
Encryption	Daten verschlüsselt sichern.	

Parameter	Bedeutung	
	<input type="checkbox"/>	Daten werden unverschlüsselt gesichert.
	<input checked="" type="checkbox"/>	Daten werden verschlüsselt gesichert.
Encryption passphrase	Verschlüsselungspasswort Das Eingabefeld ist nur sichtbar, wenn das Kontrollfeld <b>Encryption</b> markiert ist.	
Confirm passphrase	Verschlüsselungspasswort zur Kontrolle Das Eingabefeld ist nur sichtbar, wenn das Kontrollfeld <b>Encryption</b> markiert ist.	

### 3.8.1.2 Restore-Funktion

Mit der Restore-Funktion können während des Betriebes die Daten und Geräteeinstellungen von der Speicherkarte in den internen Speicher geladen werden.

Als Quellmedium kann das Netzwerk oder, wenn gesteckt, die Speicherkarte ausgewählt werden.

Wenn die Speicherkarte als Quellmedium ausgewählt ist, blinkt die LED des Speicherkartensteckplatzes während des Ladevorgangs gelb/orange.

Beim Laden der Daten werden die Dateien aus dem Verzeichnis media/sd/copy des Quellmediums in die entsprechenden Verzeichnisse des internen Speichers kopiert.

Das Gerät verfügt über eine aktive und eine inaktive Root-Partition. Die Systemsicherung wird auf die inaktive Partition gespeichert. Anschließend wird von der neu bespielten Partition gestartet. Kann der Startvorgang abgeschlossen werden, wird die neue Partition aktiv geschaltet. Anderenfalls wird beim nächsten Bootvorgang wieder von der alten aktiven Partition gebootet.

Nach dem Neustart wird das Boot-Projekt automatisch geladen und Einstellungen werden automatisch aktiv. Ob dabei das Boot-Projekt des internen Laufwerks oder der Speicherkarte geladen wird, ist abhängig von der Einstellung „Home directory on memory card enabled“. Diese Einstellung kann über die WBM-Seite „PLC Runtime Configuration“ im Register „Configuration“, Auswahl „PLC Runtime“ aufgerufen werden.

#### Hinweis

##### **Datengröße darf nicht größer als die interne Laufwerksgröße sein!**

Beachten Sie, dass die Größe der Daten in dem Verzeichnis media/sd/copy die Gesamtgröße des internen Laufwerks nicht überschreiten darf.

#### Hinweis

##### **Wiederherstellung nur vom internen Speicher möglich!**

Wenn das Produkt von der Speicherkarte gebootet wurde, ist eine Wiederherstellung der Firmware nicht möglich.

**i Hinweis****Reset durch Wiederherstellung**

Durch die Wiederherstellung des Systems, der Einstellungen oder von CODESYS wird ein Reset ausgeführt!

**i Hinweis****Verbindungsverlust durch Wiederherstellung!**

Wenn sich durch die Wiederherstellung die Parameter der ETHERNET-Verbindung ändern, kann das WBM anschließend eventuell keine Verbindung mehr zum Produkt aufbauen. Rufen Sie das WBM neu mit der korrekten IP-Adresse des Produktes in der Adresszeile auf.

**i Hinweis****Restore-Zeit berücksichtigen**

Der Restore-Vorgang benötigt ca. 2 ... 3 Minuten.

Nach dem Restore-Vorgang wird der Controller neu gestartet und ist danach wieder einsatzbereit.

Die Restore-Funktion kann über die WBM-Seite „Firmware Restore“ im Register „Configuration“, Auswahl „Package Server“ > „Firmware Restore“ aufgerufen werden.

Tabelle 99: WBM-Seite „Firmware Restore“ – Gruppe „Firmware Restore“

Parameter	Bedeutung	
Source	Datenquelle für die Wiederherstellung	
	Memory Card	Die Daten werden von der Speicherkarte gelesen. Diese Auswahl ist nur aktiv, wenn eine Speicherkarte gesteckt ist und nicht von dieser gebootet wurde.
	USB-Stick	Die Daten werden vom USB-Stick gelesen. Diese Auswahl ist nur bei Produkten mit USB-Anschluss vorhanden. Die Auswahl ist nur aktiv, wenn ein USB-Stick gesteckt ist und nicht von diesem gebootet wurde.
	Network	Die Daten werden vom PC hochgeladen und wiederhergestellt.
Boot Device	Speichermedium, von dem das Gerät gebootet wurde	
PLC Runtime Project	Name der Back-up-Datei für das CODESYS Projekt; Das Eingabefeld ist nur aktiv, wenn als Datenquelle das Netzwerk ausgewählt ist.	
Settings	Name der Back-up-Datei für die Einstellungen; Das Eingabefeld ist nur aktiv, wenn als Datenquelle das Netzwerk ausgewählt ist.	
System	Name der Back-up-Datei für die Systemdaten und das Root-Dateisystem; Das Eingabefeld ist nur aktiv, wenn als Datenquelle das Netzwerk ausgewählt ist.	
Decryption	Verschlüsselung der Daten	
	<input type="checkbox"/>	Die Daten wurden verschlüsselt gesichert.
	<input checked="" type="checkbox"/>	Die Daten wurden unverschlüsselt gesichert.

Parameter	Bedeutung
Decryption passphrase	Verschlüsselungspasswort; Das Eingabefeld ist nur sichtbar, wenn das Kontrollfeld <b>Decryption</b> markiert ist.

### 3.8.2 Speicherkartenfunktion

#### 3.8.2.1 Einfügen einer Speicherkarte im Betrieb

Der Feldbusknoten und das SPS-Programm sind in Betrieb.

Sie legen eine Speicherkarte im laufenden Betrieb ein.

Im Normalbetrieb wird die Speicherkarte als Laufwerk in das Dateisystem des Controllers eingebunden. Es werden keine automatischen Kopiervorgänge ausgelöst.

Die LED über der Speicherkarte blinkt während des Zugriffs gelb/orange.

Die Speicherkarte ist anschließend betriebsbereit und steht unter /media/sd zur Verfügung.

#### 3.8.2.2 Entfernen der Speicherkarte im Betrieb

Der Feldbusknoten und das SPS-Programm sind in Betrieb und die Speicherkarte ist gesteckt.

Sie ziehen die Speicherkarte im laufenden Betrieb heraus.

#### Hinweis

##### **Daten können beim Schreiben verloren gehen!**

Beachten Sie, dass bei dem Herausziehen der Speicherkarte während eines Schreibzugriffes Daten verloren gehen.

Die LED über der Speicherkarte blinkt während des versuchten Zugriffs gelb/orange.

Der Controller arbeitet anschließend ohne Speicherkarte.

#### 3.8.2.3 Einstellung des Home-Verzeichnisses für das Laufsystem

Standardmäßig liegt das Home-Verzeichnis für das Laufzeitsystem im internen Speicher des Controllers. Im Home-Verzeichnis wird unter anderem ein ggf. vorhandenes Boot-Projekt gespeichert.

Mit dem WBM kann das Home-Verzeichnis für das Laufzeitsystem auf die Speicherkarte verlagert werden, um beispielsweise mehr Speicherplatz für ein großes Boot-Projekt oder andere Dateien bereitzustellen.

Vor einer Umschaltung sind einige Voraussetzungen zu schaffen.

- Eine laufende IEC-61131-Anwendung muss angehalten werden und das Gerät durch Aufruf der Funktion „Reset (Ursprung)“ in den Grundzustand gebracht werden. Ein eventuell vorhandenes Boot-Projekt wird dabei gelöscht.
- Wenn das Home-Verzeichnis auf die Speicherkarte gelegt werden soll, muss eine mit einem unterstützten File-System formatierte Speicherkarte eingesteckt sein. Nur die erste Partition einer Speicherkarte ist unter /media/sd erreichbar und kann als Home-Verzeichnis benutzt werden.

Nur wenn die obigen beiden Bedingungen zutreffen, kann mit dem WBM auf der Seite „PLC Runtime“ das Kontrollfeld „Home directory on memory card enabled“ aktiviert werden. Die Einstellung wird durch Betätigen der Schaltfläche **[Submit]** übernommen und nach dem nächsten Neustart wirksam.

Es werden keine Dateien vom alten in das neue Home-Verzeichnis übernommen.

Nach der Umschaltung muss ein Projekt neu geladen und ein Boot-Projekt neu angelegt werden.

Zu beachten ist, dass die Speicherkarte unter keinen Umständen mehr entfernt werden darf, solange das Home-Verzeichnis dort liegt. Bei einer laufenden Applikation kann sonst die Anlagensicherheit durch einen unkontrollierten Absturz des Controllers gefährdet werden.

Eine Umschaltung des Home-Verzeichnisses ist wirkungslos, wenn der Controller von einer Speicherkarte gebootet wurde. Der Konfigurationszustand wird zwar gespeichert, wird aber erst wirksam, wenn der Speicherkarteninhalt in den internen Speicher kopiert wird.

### 3.8.2.4 Boot-Projekt laden

Ein eventuell vorhandenes Boot-Projekt wird abhängig von der Einstellung des Home-Verzeichnisses für das Laufzeitsystem geladen. Die nachfolgende Tabelle zeigt die möglichen Ergebnisse an:

Tabelle 100: Laden eines Boot-Projekts

Boot-Projekt im internen Flash gespeichert	Speicherkarte mit Boot-Projekt gesteckt	„Home directory on memory card enabled“ markiert	Boot-Projekt wird geladen ...
Nein	Nein	Nein	Nein, kein Bootprojekt vorhanden
		Ja	Nein, kein Bootprojekt vorhanden
	Ja	Nein	Nein, kein Bootprojekt im internen Flash vorhanden
		Ja	Ja, von Speicherkarte
Ja	Nein	Nein	Ja, aus internem Flash
		(Ja) Unzulässig	Nein, unzulässige Kombination, da für diese Einstellung kein Boot-Projekt im internen Flash vorhanden sein darf
	Ja	Nein	Ja, aus internem Flash
		(Ja) Unzulässig	Nein, unzulässige Kombination, da für diese Einstellung kein Boot-Projekt im internen Flash vorhanden sein darf

## 3.9 Diagnosefunktionen

### 3.9.1 Diagnose über Anzeigeelemente

Verschiedene Anzeigeelemente am Produkt ermöglichen eine direkte Diagnose, z. B. LEDs für Spannungsversorgung, System, Feldbus und Netzwerk.

Die Anzahl und Ausprägung der Anzeigeelemente ist produktabhängig. Die Diagnosen über diese Anzeigeelemente sind in den jeweiligen Produkthandbüchern beschrieben.

Die in den folgenden Abschnitten beschriebenen Blinksequenzen gelten für alle Produkte, die im Gültigkeitsbereich dieses Dokuments aufgelistet sind.

### 3.9.1.1 Diagnose über Blinksequenzen

#### Ablauf der Blinksequenzen

Eine Diagnose (Störung) wird immer zyklisch mit drei Blinksequenzen dargestellt:

1. Die erste Blinksequenz leitet durch Flackern (10 Hz) die Ausgabe des Fehlercodes und des Fehlerargumentes ein.
2. Die zweite Blinksequenz blinkt (1 Hz) den Fehlercode aus.
3. Die dritte Blinksequenz blinkt (1 Hz) das Fehlerargument aus.

#### Beispiel einer Diagnosemeldung über Blinksequenzen

Folgendes Beispiel verdeutlicht die Darstellung einer Diagnosemeldung mittels Blinksequenzen. Die LED „I/O“ zeigt einen Datenfehler am Lokalbus an. Der Datenfehler wird durch das Entfernen eines I/O-Moduls verursacht, das sich an der 6. Position des Busknotens befindet.

#### Einleitung der Startphase

1. Die LED „I/O“ blinkt 1 Zyklus von ca. 10 Hz.
2. Es folgt eine Pause von ca. 1 Sekunde.

#### Fehlercode 4: Datenfehler am Lokalbus

3. Die LED „I/O“ blinkt 4 Zyklen von ca. 1 Hz.
4. Es folgt eine Pause von ca. 1 Sekunde.

#### Fehlerargument 5: I/O-Modul auf dem 6. Steckplatz

5. Die LED „I/O“ blinkt 5 Zyklen von 1 Hz. Dies bedeutet, dass am Lokalbus nach dem 5. I/O-Modul eine Unterbrechung aufgetreten ist.
6. Die Blinksequenz startet mit dem Flackern die erneute Einleitung der Startphase. Bei nur einer Störung wiederholt sich dieser Ablauf.

#### 3.9.1.1.1 Fehlercodes der I/O-LED

Tabelle 101: Übersicht Fehlercodes LED "I/O"

Fehlercode	Bedeutung
1	Hardware- und Konfigurationsfehler
2	Konfigurationsfehler
3	Lokalbus-Protokollfehler
4	Physischer Fehler am Lokalbus
5	Lokalbus-Initialisierungsfehler
6	Nicht verwendet
7	Nicht unterstütztes I/O-Modul
8	Nicht verwendet
9	CPU-Ausnahmefehler

## Fehlercode 1 - Hardware- und Konfigurationsfehler

Tabelle 102: Fehlercode 1 - Hardware- und Konfigurationsfehler: Bedeutung der Blinkcodes und Maßnahmen zur Fehlerbehebung

Fehlerargument	Ursache	Abhilfe
-	Ungültige Parameterprüfsumme der Lokalbus-Schnittstelle	<ol style="list-style-type: none"> <li>1. Schalten Sie die Versorgungsspannung des Controllers ab.</li> <li>2. Wechseln Sie den Controller aus.</li> <li>3. Schalten Sie die Versorgungsspannung wieder ein.</li> </ol>
1	Während der Inlinedegenerierung hat der interne Pufferspeicher die max. Datenmenge überschritten.	<ol style="list-style-type: none"> <li>1. Schalten Sie die Versorgungsspannung des Controllers ab.</li> <li>2. Reduzieren Sie die Anzahl der I/O-Module.</li> <li>3. Schalten Sie die Versorgungsspannung wieder ein.</li> </ol>
2	I/O-Modul(e) mit nicht unterstütztem Datentyp	<ol style="list-style-type: none"> <li>1. Aktualisieren Sie die Firmware des Controllers. Bleibt der Fehler bestehen, liegt ein Fehler an einem I/O-Modul vor. Ermitteln Sie dieses wie folgt:</li> <li>2. Schalten Sie die Versorgungsspannung des Controllers ab.</li> <li>3. Platzieren Sie das Endmodul in der Mitte der angeschlossenen I/O-Module.</li> <li>4. Schalten Sie die Versorgungsspannung wieder ein.</li> <li>5. Falls die LED noch rot blinkt, schalten Sie die Versorgungsspannung erneut aus und platzieren Sie das Endmodul in der Mitte der ersten Hälfte der I/O-Module (zum Controller hin).</li> <li>6. Wenn die LED nicht mehr blinkt, schalten Sie die Versorgungsspannung ab und platzieren Sie das Endmodul in der Mitte der zweiten Hälfte der I/O-Module (vom Controller weg).</li> <li>7. Schalten Sie die Versorgungsspannung wieder ein.</li> <li>8. Wiederholen Sie diese Prozedur so oft, bis Sie das defekte I/O-Modul ermittelt haben. Tauschen Sie dieses anschließend aus.</li> </ol>
3	Unbekannter Modultyp des Flashprogrammspeichers	<ol style="list-style-type: none"> <li>1. Schalten Sie die Versorgungsspannung des Controllers ab.</li> <li>2. Wechseln Sie den Controller aus.</li> <li>3. Schalten Sie die Versorgungsspannung wieder ein.</li> </ol>
4	Fehler beim Beschreiben des Flash-Speichers aufgetreten	<ol style="list-style-type: none"> <li>1. Schalten Sie die Versorgungsspannung des Controllers ab.</li> <li>2. Wechseln Sie den Controller aus.</li> <li>3. Schalten Sie die Versorgungsspannung wieder ein.</li> </ol>
5	Fehler beim Löschen eines Flashsektors aufgetreten	-
6	Die I/O-Modulkonfiguration nach einem Lokalbusreset stimmt nicht mit der I/O-Modulkonfiguration nach dem letzten Start des Controllers überein.	<ul style="list-style-type: none"> <li>Starten Sie den Controller neu, indem Sie die Versorgungsspannung abschalten und anschließend wieder einschalten oder die Reset-Taste auf dem Controller drücken.</li> </ul>
7	Fehler beim Beschreiben des seriellen EEPROM aufgetreten	<ol style="list-style-type: none"> <li>1. Schalten Sie die Versorgungsspannung des Controllers ab.</li> <li>2. Wechseln Sie den Controller aus.</li> <li>3. Schalten Sie die Versorgungsspannung wieder ein.</li> </ol>
8	Unzulässige Hardware-/Firmwarekombination	-
9	Ungültige Prüfsumme im seriellen EEPROM	-
10	Initialisierung des seriellen EEPROM fehlgeschlagen	-

Fehlerargument	Ursache	Abhilfe
11	Fehler beim Lesezugriff auf dem seriellen EEPROM aufgetreten	<ol style="list-style-type: none"> <li>Schalten Sie die Versorgungsspannung des Controllers ab.</li> <li>Reduzieren Sie die Anzahl der I/O-Module.</li> <li>Schalten Sie die Versorgungsspannung wieder ein.</li> </ol>
12	Zeit für Zugriff auf dem seriellen EEPROM überschritten	<ol style="list-style-type: none"> <li>Schalten Sie die Versorgungsspannung des Controllers ab.</li> <li>Wechseln Sie den Controller aus.</li> <li>Schalten Sie die Versorgungsspannung wieder ein.</li> </ol>
14	Maximale Anzahl an Gateway- oder Mailboxmodulen überschritten	<ol style="list-style-type: none"> <li>Schalten Sie die Versorgungsspannung des Controllers ab.</li> <li>Reduzieren Sie die Anzahl der Gateway- oder Mailboxmodule.</li> <li>Schalten Sie die Versorgungsspannung wieder ein.</li> </ol>
16	Maximale Anzahl an I/O-Modulen überschritten	<ol style="list-style-type: none"> <li>Schalten Sie die Versorgungsspannung des Controllers ab.</li> <li>Reduzieren Sie die Anzahl der I/O-Module.</li> <li>Schalten Sie die Versorgungsspannung wieder ein.</li> </ol>

### Fehlercode 2 - Konfigurationsfehler

Tabelle 103: Fehlercode 2 - Konfigurationsfehler: Bedeutung der Blinkcodes und Maßnahmen zur Fehlerbehebung

Fehlerargument	Ursache	Abhilfe
2	Maximalgröße des Prozessab-bilds überschritten	<ol style="list-style-type: none"> <li>Schalten Sie die Versorgungsspannung des Controllers ab.</li> <li>Reduzieren Sie die Anzahl der I/O-Module.</li> <li>Schalten Sie die Versorgungsspannung wieder ein.</li> </ol>

### Fehlercode 3 - Lokalbus-Protokollfehler

Tabelle 104: Fehlercode 3 - Lokalbus-Protokollfehler: Bedeutung der Blinkcodes und Maßnahmen zur Fehlerbehebung

Fehlerargument	Ursache	Abhilfe
-	Störung der Lokalbuskommuni-kation; defektes I/O-Modul kann nicht ermittelt werden.	<ul style="list-style-type: none"> <li>✓ Ist am Controller ein Potentialeinspeisemodul (z. B. 750-602) angeschlossen, stellen Sie sicher, dass dieses funktioniert. Ist das Einspeisemodul fehlerfrei, dann liegt eine Störung an einem I/O-Modul vor. Ermitteln Sie dieses I/O-Modul wie folgt: <ol style="list-style-type: none"> <li>Schalten Sie die Versorgungsspannung des Controllers ab.</li> <li>Platzieren Sie das Endmodul in der Mitte der angeschlossenen I/O-Module.</li> <li>Schalten Sie die Versorgungsspannung wieder ein.</li> <li>Falls die I/O-LED noch rot blinkt, schalten Sie die Versorgungsspannung erneut aus und platzieren Sie das Endmodul in der Mitte der ersten Hälfte der I/O-Module (zum Controller hin).</li> </ol> </li> <li>✓ Wenn nur noch ein I/O-Modul übrig ist, aber die LED noch blinkt, dann ist dieses oder die Lokalbusschnittstelle des Controllers defekt. Tauschen Sie das I/O-Modul oder den Controller aus: <ol style="list-style-type: none"> <li>Wenn die LED nicht mehr blinkt, schalten Sie die Versorgungsspannung ab und platzieren Sie das Endmodul in der Mitte der zweiten Hälfte der I/O-Module (vom Controller weg).</li> <li>Schalten Sie die Versorgungsspannung wieder ein.</li> <li>Wiederholen Sie diese Prozedur so oft, bis Sie das defekte I/O-Modul ermittelt haben. Tauschen Sie dieses anschließend aus.</li> </ol> </li> </ul>

## Fehlercode 4 - Physischer Fehler am Lokalbus

Tabelle 105: Fehlercode 4 - Physischer Fehler am Lokalbus: Bedeutung der Blinkcodes und Maßnahmen zur Fehlerbehebung

Fehlerargument	Ursache	Abhilfe
-	Anzahl der zulässigen I/O-Module überschritten	<ol style="list-style-type: none"> <li>1. Schalten Sie die Versorgungsspannung des Controllers ab.</li> <li>2. Reduzieren Sie die Anzahl der I/O-Module auf einen zulässigen Wert.</li> <li>3. Schalten Sie die Versorgungsspannung wieder ein.</li> </ol>
n*	Lokalbusunterbrechung nach dem n-ten I/O-Modul mit Prozessdaten.	<ol style="list-style-type: none"> <li>1. Schalten Sie die Versorgungsspannung des Controllers ab.</li> <li>2. Tauschen Sie das (n+1)-te I/O-Modul mit Prozessdaten aus.</li> <li>3. Schalten Sie die Versorgungsspannung wieder ein.</li> </ol> <p>*) I/O-Module, die keine Prozessdaten liefern, werden nicht beachtet (z. B. Einspeisemodul ohne Diagnose).</p>

## Fehlercode 5 - Lokalbus-Initialisierungsfehler

Tabelle 106: Fehlercode 5 - Lokalbus-Initialisierungsfehler: Bedeutung der Blinkcodes und Maßnahmen zur Fehlerbehebung

Fehlerargument	Ursache	Abhilfe
n*	Fehler in der Registerkommunikation während der Lokalbusinitialisierung	<ol style="list-style-type: none"> <li>1. Schalten Sie die Versorgungsspannung des Controllers ab.</li> <li>2. Tauschen Sie das (n+1)-te I/O-Modul mit Prozessdaten aus.</li> <li>3. Schalten Sie die Versorgungsspannung wieder ein.</li> </ol> <p>*) I/O-Module, die keine Prozessdaten liefern, werden nicht beachtet (z. B. Einspeisemodul ohne Diagnose).</p>

## Fehlercode 7 - Nicht unterstütztes I/O-Modul

Tabelle 107: Fehlercode 7 - Nicht unterstütztes I/O-Modul: Bedeutung der Blinkcodes und Maßnahmen zur Fehlerbehebung

Fehlerargument	Ursache	Abhilfe
n	Erstes nicht unterstütztes I/O-Modul an Stelle n	<ol style="list-style-type: none"> <li>1. Schalten Sie die Versorgungsspannung des Controllers ab.</li> <li>2. Tauschen Sie das n-te I/O-Modul mit Prozessdaten aus bzw. reduzieren Sie die Anzahl der I/O-Module auf n-1.</li> <li>3. Schalten Sie die Versorgungsspannung wieder ein.</li> </ol>

## Fehlercode 9 - CPU-Ausnahmefehler

Tabelle 108: Fehlercode 9 - CPU-Ausnahmefehler: Bedeutung der Blinkcodes und Maßnahmen zur Fehlerbehebung

Fehlerargument	Ursache	Abhilfe
1	Ungültige Programmanweisung	Störung der Programmabfolge - <ul style="list-style-type: none"> <li>▪ Kontaktieren Sie den WAGO-Support.</li> </ul>
2	Überlauf Stapelspeicher	Störung der Programmabfolge <ul style="list-style-type: none"> <li>▪ Kontaktieren Sie den WAGO-Support.</li> </ul>
3	Unterlauf Stapelspeicher	Störung der Programmabfolge <ul style="list-style-type: none"> <li>▪ Kontaktieren Sie den WAGO-Support.</li> </ul>
4	Ungültiges Ereignis (NMI)	Störung der Programmabfolge <ul style="list-style-type: none"> <li>▪ Kontaktieren Sie den WAGO-Support.</li> </ul>

Fehlerargument	Ursache	Abhilfe
5	Lokalbuswatchdog hat angesprochen.	<ul style="list-style-type: none"> <li>✓ Bei CODESYS-Applikationen:                             <ul style="list-style-type: none"> <li>▪ Kontaktieren Sie den WAGO-Support.</li> </ul> </li> <li>✓ Bei C-Applikationen:                             <ul style="list-style-type: none"> <li>▪ Prüfen Sie die Einstellungen der Zeitüberwachung.</li> </ul> </li> </ul>

### 3.9.1.1.2 Fehlercodes der MS-LED

Tabelle 109: Übersicht Fehlercodes LED "MS"

Fehlercode	Bedeutung
1	Konfigurationsfehler

Tabelle 110: Fehlercode 1 - Konfigurationsfehler: Bedeutung der Blinkcodes und Maßnahmen zur Fehlerbehebung

Fehlerargument	Ursache	Abhilfe
5	Fehler beim Abgleich der Steuerungskonfiguration mit dem Lokalbus	<ol style="list-style-type: none"> <li>1. Überprüfen Sie die Angabe der gesteckten I/O-Module in der CODESYS Steuerungskonfiguration.</li> <li>2. Gleichen Sie diese mit den tatsächlich gesteckten I/O-Modulen ab.</li> <li>3. Übersetzen Sie das Projekt erneut.</li> <li>4. Laden Sie das Projekt wieder in den Controller.</li> </ol>

### 3.9.2 Diagnose über WBM

Tabelle 111: WBM-Seite „Log Message Viewer“ – Gruppe „Refresh Options“

Parameter	Bedeutung	
Read only the last	Anzeige der letzten n Meldungen einschalten/ausschalten; Anzahl der angezeigten Meldungen eingeben	
Automatic refresh interval (sec)	Zyklische Aktualisierung einschalten/ausschalten; Zykluszeit in Sekunden eingeben, mit der eine zyklische Aktualisierung durchgeführt wird; Abhängig vom Status wechselt die Beschriftung der Schaltfläche („Refresh“/„Start“/„Stop“).	
Source	Quelle der Diagnosemeldungen auswählen; Die Drop-Down-Liste ist abhängig vom angemeldeten Benutzer.	
	user	Nur Standard-Diagnosemeldungen
	admin	Standard-Diagnosemeldungen und alle Log-Dateien im Ordner <code>/var/log/*</code>

Tabelle 112: WBM-Seite „Download“ – Gruppe „Diagnostic Information“

Parameter	Bedeutung
[Download]	Diagnoseinformationen vom Gerät herunterladen

Tabelle 113: WBM-Seite „Network Capture“ – Gruppe „State“

Parameter	Bedeutung
Current State	Aktueller Status der Netzwerkaufzeichnung
Last Captured Package Count	Bereits aufgezeichnete Netzwerkpakete
Last Refresh Time	Zeitpunkt der letzten Aktualisierung von „Current State“ und „Last Captured Package Count“

Tabelle 114: WBM-Seite „Network Capture“ – Gruppe „Configuration“

Parameter	Bedeutung	
Enable	Aufzeichnung einschalten/ausschalten	
Rotate Log Files	Rotierendes Aufzeichnen einschalten/ausschalten; Wenn diese Option eingeschaltet ist, wird der Netzwerkverkehr in bis zu drei Dateien mit der eingestellten maximalen Dateigröße abgespeichert. Ist die maximale Dateigröße der ersten Datei erreicht, werden die Daten in einer zweiten Datei weiter aufgezeichnet usw. Ist auch die maximale Dateigröße der dritten Datei erreicht, werden die Daten der ersten Datei überschrieben.	
Max. Filesize	Maximale Dateigröße für die Datenaufzeichnung eingeben	
Storage Location	Speicherort für die aufgezeichneten Daten auswählen	
	Internal Flash	Die Daten werden im internen Speicher gespeichert.
	SD-Card	Die Daten werden auf der Speicherkarte gespeichert. Wenn „SD-Card“ ausgewählt ist, aber die Speicherkarte nicht mehr gesteckt ist, dann ist diese Option nicht mehr aktiv und nur noch „Internal-Flash“ auswählbar.
Listen On Network Interface	Netzwerkinterface auswählen, von welchem der Netzwerkverkehr mitgeschnitten werden soll; Zur Auswahl stehen dabei die verfügbaren Netzwerkschnittstellen des Gerätes.	

Tabelle 115: WBM-Seite „Network Capture“ – Gruppe „Filter Configuration“

Parameter	Bedeutung
Capture Filter	Aufzeichnungsfilter eingegeben; Diese dienen dazu, nur den relevanten bzw. gewünschten Datenverkehr mitzuschneiden. So ist es bspw. möglich, nur die Kommunikation von nur einem Port aufzuzeichnen oder von einer bestimmten IP-Adresse. Weitere Informationen zu den möglichen Filtereinstellungen finden Sie in den Erläuterungen der „Capture Filter“ in der Dokumentation zu „Wireshark“.

Tabelle 116: WBM-Seite „Network Capture“ – Gruppe „Log Download“

Parameter	Bedeutung
Select Log File	Mitschnitt auswählen, der vom Produkt heruntergeladen werden soll

# 4 In Betrieb nehmen

## 4.1 Einschalten des Controllers

Überprüfen Sie vor Einschalten des Controllers, dass Sie

- den Controller ordnungsgemäß montiert haben (siehe Kapitel „Montieren“),
- alle benötigten Datenleitungen (siehe Kapitel „Anschlüsse“) an die entsprechenden Schnittstellen angeschlossen und mit den an den Steckverbindern vorhandenen Arretierungsschrauben befestigt haben,
- die System- und Feldversorgung angeschlossen haben (siehe Systembeschreibung),
- das Endmodul gesteckt haben (siehe Systembeschreibung),
- einen angemessenen Potentialausgleich an Ihrer Maschine/Anlage durchgeführt haben (siehe Systembeschreibung) und
- die Schirmung ordnungsgemäß durchgeführt haben (siehe Systembeschreibung).

Zum Einschalten des Controllers und der daran angeschlossenen I/O-Module schalten Sie an Ihrem Netzteil die Versorgungsspannung ein.

Das Starten des Controllers wird durch ein kurzes Aufleuchten aller LEDs signalisiert.

Nach einigen weiteren Sekunden signalisiert die SYS-LED den erfolgreichen Bootvorgang des Controllers.

Gleichzeitig wird das Laufzeitsystem CODESYS V3 gestartet.

Wurde das gesamte System erfolgreich gestartet, leuchten die SYS und die I/O-LED grün.

Wenn ein ausführbares IEC-61131-3-Programm im Controller gespeichert ist und gestartet wurde, leuchtet die RUN-LED grün.

Wenn kein ausführbares Programm im Controller gespeichert ist oder der Betriebsartenschalter auf STOP steht, wird dies ebenfalls durch RUN-LED angezeigt (siehe Diagnose über LED-Anzeigen System/Feldbus).

## 4.2 Ermitteln der IP-Adresse des Host-PC

Damit der Host-PC mit dem Controller über das ETHERNET-Netzwerk kommunizieren kann, müssen sich Host-PC und Controller im gleichen Subnetz befinden.

Zum Ermitteln der IP-Adresse des Host-PC (mit Betriebssystem Microsoft Windows®) mittels der Eingabeaufforderung gehen Sie folgendermaßen vor:

1. Öffnen Sie die Eingabeaufforderung. Geben Sie dazu im Eingabefeld unter **Start > Windows-System > Ausführen** (Windows® 10) oder **Start > Programme/Dateien durchsuchen** (Windows® 7) den Befehl „cmd“ ein.
  2. Bestätigen Sie die Eingabe mit der Schaltfläche **[OK]** oder der **Enter**-Taste.
  3. Geben Sie in der Eingabeaufforderung den Befehl „ipconfig“ ein.
  4. Bestätigen Sie die Eingabe mit der **Enter**-Taste.
- ➔ Es erscheinen die IP-Adresse, Subnetzmaske und das Standard-Gateway mit den dazugehörigen Parametern.

### 4.3 Einstellen einer IP-Adresse

Im Auslieferungszustand des Produktes ist für die ETHERNET-Schnittstelle (Port X1 und Port X2) folgende IP-Adressierung aktiv:

Tabelle 117: Voreingestellte IP-Adressierung der ETHERNET-Schnittstellen

ETHERNET-Schnittstelle	Voreinstellung
X1/X2 (Switched Mode)	Dynamische Vergabe der IP-Adresse mittels DHCP (Dynamic Host Configuration Protocol)

- Passen Sie mit einem der vorhandenen Konfigurationswerkzeuge (z. B. WBM oder WAGO Ethernet Settings) die IP-Adressierung an Ihre Systemstruktur an, damit ein PC und das Produkt miteinander kommunizieren können, siehe [🔗 Konfigurieren \[► 89\]](#).

#### Beispiel zum Einbinden des Produktes (192.168.1.17) in ein bestehendes Netzwerk:

- Die IP-Adresse des Host-PCs lautet **192.168.1.2**.
- Produkt und Host-PC müssen im gleichen Subnetz sein (unabhängig von der IP-Adresse des Host-PCs).
- Die ersten drei Stellen der IP-Adresse des Host-PCs und des Produktes müssen bei einer Subnetzmaske von **255.255.255.0** übereinstimmen, damit sich beide im gleichen Subnetz befinden.

Tabelle 118: Netzmaske 255.255.255.0

Host-PC	Subnetzadressraum für das Produkt
192.168.1.2	192.168.1.1 oder 192.168.1.3 ... 192.168.1.254

#### 4.3.1 IP-Verbindung über USB (PFC300)

Zur Inbetriebnahme und zu Service-Zwecken können Sie eine IP-Verbindung über USB aufbauen.

1. Verbinden Sie den Controller über die USB-Service-Schnittstelle und ein USB-Service-Kabel mit Ihrem PC.
2. Wenn Sie Windows® 10 einsetzen, gehen Sie weiter zu Schritt 4.
  - ⇒ Unter Windows® 7 verhält sich der Controller nach dem Anschließen wie ein externes Laufwerk. Auf dem Laufwerk ist ein Treiber für die IP-Verbindung über USB gespeichert.
3. Installieren Sie diesen Treiber.
  - ⇒ Anschließend ist die Kommunikation über die IP-Verbindung über USB möglich.
4. Rufen Sie im Browser die feste IP-Adresse des Produktes 192.168.42.42 auf.
  - ➔ Das Web-Based-Management des Controllers wird geöffnet.
  - ➔ Sie können damit alle erforderlichen Einstellungen am Controller durchführen.

#### 4.3.2 Einstellen einer IP-Adresse über das WBM

Sie können die IP-Adresse des Controllers ohne weitere Tools direkt über das eingebaute Web-Based-Management ändern.

1. Verbinden Sie den Controller und Ihren PC mit einem geeigneten Netzkabel.
2. Starten Sie einen Internetbrowser auf dem PC.

3. Rufen Sie das WBM auf dem Controller auf. Geben Sie dazu in der Eingabezeile des Browsers folgendes ein: „https://<IP-Adresse>/wbm“.
4. Wenn Sie die IP-Adresse nicht kennen, ermitteln Sie die IP-Adresse wie weiter vorne beschrieben.
  - ⇒ Sie werden anschließend aufgefordert, sich zu authentifizieren.
5. Geben Sie den Benutzernamen „user“ und das entsprechende Passwort (im Auslieferungszustand „user“) ein.
  - ⇒ Wenn Sie das Standardpasswort noch nicht geändert haben, werden Sie aufgefordert, das Passwort jetzt zu ändern.
6. Öffnen Sie das Register „Configuration“.
7. Wählen Sie in der Navigation den Punkt „Networking“ und den Unterpunkt „TCP/IP Configuration“.
8. Wählen Sie in der Gruppe „TCP/IP Configuration“ im Auswahlfeld „IP Source“ den Eintrag „Static IP“.
9. Geben Sie im Eingabefeld „Static IP Address“ die gewünschte IP-Adresse ein.
10. Geben Sie im Eingabefeld „Subnet Mask“ die gewünschte Subnetzmaske ein.
11. Um die Änderungen zu bestätigen, klicken Sie auf die Schaltfläche **[Submit]**.
  - ⇒ Durch die Änderung der IP-Adresse wird die Verbindung zum Controller unterbrochen.
12. Stellen Sie eine neue Verbindung mit der geänderten IP-Adresse her.

#### 4.3.3 Zuweisen einer IP-Adresse mit DHCP

Der Controller kann seine IP-Adresse dynamisch (DHCP) von einem Server beziehen. Im Gegenteil zu festen IP-Adressen werden dynamisch zugewiesene Adressen nicht permanent gespeichert. Daher ist bei jedem Neustart des Controllers die Anwesenheit eines DHCP-Servers erforderlich.

Wurde die IP-Adresse mittels DHCP vergeben (Standardeinstellung), so kann diese über die Einstellungen bzw. die Ausgaben des jeweiligen DHCP-Servers ermittelt werden.

In Verbindung mit einem an das DHCP angebenen DNS-Server ist es möglich, das Gerät über seinen Hostnamen zu erreichen. Dieser besteht aus einem Präfix und der MAC-Adresse bzw. einem Teil davon. Die MAC-Adresse des Produktes ist auf dem seitlich am Produkt angebrachten Etikett aufgedruckt.

#### 4.3.4 Ändern einer IP-Adresse mit "WAGO Ethernet Settings"

Die Microsoft-Windows®-Anwendung „WAGO Ethernet Settings“ ist eine Software, mit welcher Sie den Controller identifizieren und die Netzwerkeinstellungen konfigurieren können.

Zur Datenkommunikation können Sie das WAGO USB-Service-Kabel oder ggf. das IP-Netzwerk verwenden.

1. Schalten Sie die Betriebsspannung des Controllers aus.
2. Stellen Sie eine geeignete Verbindung zwischen dem Controller und Ihrem PC her.
3. Schalten Sie die Betriebsspannung des Controllers wieder ein.
4. Starten Sie das Programm „WAGO Ethernet Settings“.

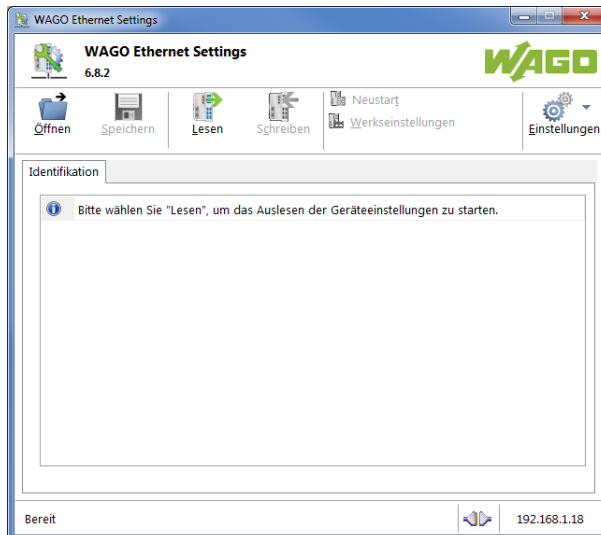


Abbildung 6: WAGO Ethernet Settings – Startbildschirm (Beispielbild)

5. Klicken Sie auf die Schaltfläche **[Lesen]**, um den angeschlossenen Controller einzulesen und zu identifizieren.
6. Wählen Sie das Register **„Netzwerk“**:

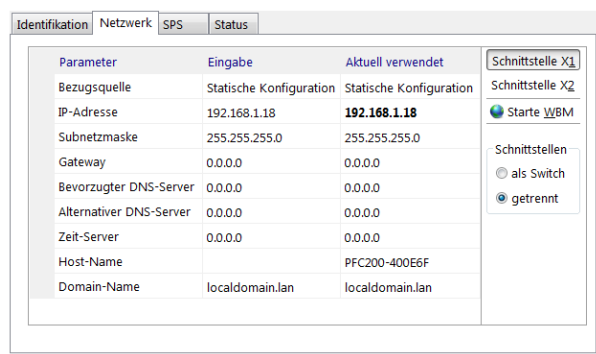


Abbildung 7: WAGO Ethernet Settings – Register Netzwerk (Beispielbild)

7. Damit Sie eine feste Adresse vergeben können, wählen Sie in der Zeile **„Bezugsquelle“** unter **„Eingabe“** den Wert „Statische Konfiguration“ aus. Standardmäßig ist DHCP aktiviert.
8. Geben Sie in der Spalte **„Eingabe“** die gewünschte IP-Adresse und gegebenenfalls die Adresse der Subnetzmaske und des Gateways ein.
9. Klicken Sie auf die Schaltfläche **[Schreiben]**, um die Adresse in den Controller zu übernehmen. (Gegebenenfalls wird „WAGO Ethernet Settings“ Ihren Controller automatisch neu starten. Diese Aktion kann ca. 30 Sekunden in Anspruch nehmen.)
10. Nun können Sie „WAGO Ethernet Settings“ schließen oder bei Bedarf direkt im Web-Based-Management weitere Einstellungen vornehmen. Klicken Sie dazu auf die Schaltfläche **[Starte WBM]** im rechten Fensterbereich.

#### 4.3.5 IP-Adressvorgabe mit Adresswahlschalter einstellen

Bei Produkten mit einem Adresswahlschalter können Sie mit diesem Schalter die Netzwerkeinstellungen verändern.

Der Adresswahlschalter umfasst 8 Einzelschalter 1 ... 8 mit den Wertigkeiten 1 ... 128. Ein ausgeschalteter Schalter hat den Wert 0. Der eingestellte Adresswert ergibt sich aus der Summe der Wertigkeit aller eingeschalteten Schalter (Beispiel: Schalter 7, 6 und 3 auf „ON“ entspricht Adresswert  $64 + 32 + 4 = 100$ ). Damit können Sie einen Adresswert von 0 ... 255 einstellen.

Die Einstellung des Adresswahlschalters wird nur beim Neustart des Controllers abgefragt. Änderungen der Schalterstellungen während des Betriebs werden bis zum nächsten Neustart ignoriert.

Wenn Sie die ETHERNET-Schnittstellen X1 und X2 im Separated Modus betreiben, wirken sich die Einstellungen nur auf die Schnittstelle X1 aus. Für die Schnittstelle X2 bleiben alle Einstellungen unverändert. Wenn Sie die ETHERNET-Schnittstellen X1 und X2 im Switched Modus betreiben, gelten die Einstellungen sowohl für die Schnittstelle X1 als auch die Schnittstelle X2.

Die folgende Tabelle zeigt die Bedeutung der Adresswerte des Adresswahlschalters.

Tabelle 119: Adresswahlschalter

Adresswert	Bedeutung
0	Die Konfiguration der IP-Parameter wird über die Einstellungen im Web-Based-Management (WBM) oder durch die Werkseinstellung vorgenommen.
1 ... 254	Es wird eine feste IP-Adresse vergeben. Die IP-Adresse setzt sich zusammen aus der Netzadresse und dem eingestellten Adresswert. Die Netzadresse ist über das WBM konfigurierbar und lautet im Auslieferungszustand 192.168.1.0 (Subnetmaske 255.255.255.0, Standardgateway 0.0.0.0).
255	Die Konfiguration der IP-Parameter wird mittels DHCP-Protokoll vorgenommen.

Beispiele:

Die eingestellte IP-Adresse ist 192.168.129.129, der Adresswahlschalter ist auf den Wert 203 eingestellt.

Wenn die Netzmaske 255.255.255.0 ist, wird der komplette vierte Wert der IP-Adresse ersetzt:

Eingestellte Netzmaske:	255 . 255 . 255 . 000
Eingestellte IP-Adresse:	192 . 168 . 129 . 129
Resultierende Netzwerkadresse:	192 . 168 . 129 . 000
Resultierende Geräteadresse:	--- . --- . --- . 129
Adresswahlschalter:	--- . --- . --- . 203
Netzwerkadresse nach Neustart:	192 . 168 . 129 . 000
Geräteadresse nach Neustart:	--- . --- . --- . 203
IP-Adresse nach Neustart:	192 . 168 . 129 . 203

Es sind 254 Adressen möglich und einstellbar (1 ... 254).

Ist die Netzmaske größer (z. B. 255.255.255.240), wird der Adresswert begrenzt. Es wird nur ein Teil der DIP-Schalter des Adresswahlschalters berücksichtigt. Für das nachfolgende Beispiel sind das nur die Schalter 1 ... 4. Die Stellung der Schalter 5 ... 8 wird ignoriert:

Eingestellte Netzmaske:	255 . 255 . 255 . 240
Eingestellte IP-Adresse:	192 . 168 . 129 . 129
Resultierende Netzwerkadresse:	192 . 168 . 129 . 128

Resultierende Geräteadresse:	---.---.---.001
Adresswahlschalter:	---.---.---.203
Netzwerkadresse nach Neustart:	192.168.129.128
Geräteadresse nach Neustart:	---.---.---.011
IP-Adresse nach Neustart:	192.168.129.139

Es sind 254 Adressen einstellbar (1 ... 254), aber nur 14 Adressen (1 ... 14) möglich.

Ist die Netzmaske kleiner (z. B. 255.255.240.000), erhöht sich die mögliche Anzahl der Geräte an einem Subnetz, aber mit dem Adresswahlschalter kann nur ein Teil der möglichen Geräteadressen eingestellt werden:

Eingestellte Netzmaske:	255.255.240.000
Eingestellte IP-Adresse:	192.168.129.129
Resultierende Netzwerkadresse:	192.168.128.000
Resultierende Geräteadresse:	---.---.---.1.129
Adresswahlschalter:	---.---.---.203
Netzwerkadresse nach Neustart:	192.168.128.000
Geräteadresse nach Neustart:	---.---.---.203
IP-Adresse nach Neustart:	192.168.128.203

Es sind 4094 Adressen möglich (1 ... 4094), aber nur 254 Adressen einstellbar (1 ... 254).

#### 4.3.6 Temporär feste IP-Adressen einstellen

Mit diesem Vorgang werden die IP-Adressen für die Netzwerkschnittstellen X1 ... X<n> temporär auf feste IP-Adressen eingestellt.

Für jede verwendete Bridge wird dabei den zugeordneten Schnittstellen eine eigene Adresse vergeben, wobei Bridge 1 die IP-Adresse „192.168.1.17“, Bridge 2 die IP-Adresse „192.168.2.17“ usw. erhält.

Es wird kein Reset durchgeführt.

Um temporär feste IP-Adressen einzustellen, gehen Sie folgendermaßen vor:

1. Bringen Sie den Betriebsartenschalter in die STOP-Position.
  2. Betätigen Sie den Reset-Taster länger als 8 Sekunden.
- ➔ Die Ausführung wird durch eine orange blinkende „SYS“-LEDs signalisiert.

Wenn Sie nach dem Aktivieren der temporären IP-Adressen Änderungen an der IP-Konfiguration einer Bridge vornehmen, werden die neuen Einstellungen permanent übernommen und sofort angewendet. Die konfigurierte Bridge verlässt somit den temporären IP-Adressmodus. Die anderen Bridges behalten bis zum Neustart/Reset die temporär eingestellte IP-Adresse.

Um die Einstellung wieder aufzuheben, gehen Sie folgendermaßen vor:

- Führen Sie einen Software-Reset durch,
- oder
- Schalten sie das Produkt aus und wieder ein.

## 4.4 Testen der Netzwerkverbindung

Um zu überprüfen, ob Sie den Controller unter der von Ihnen vergebenen IP-Adresse im Netzwerk erreichen, führen Sie den Netzwerkdienst „ping“ durch:

1. Öffnen Sie die Eingabeaufforderung. Geben sie dazu im Eingabefeld unter **Start > Windows-System > Ausführen** (Windows® 10) oder **Start > Programme/Dateien durchsuchen** (Windows® 7) den Befehl „cmd“ ein.
2. Bestätigen Sie die Eingabe mit der Schaltfläche **[OK]** oder der **Enter**-Taste.
3. Geben Sie in der Eingabeaufforderung den Befehl „ping“ und die IP-Adresse des Controllers (z. B. ping 192.168.1.17) ein.
4. Bestätigen Sie die Eingabe mit der **Enter**-Taste.
  - ⇒ Ihr PC sendet eine Anfrage, die vom Controller beantwortet wird. Die Antwort erscheint in der Eingabeaufforderung. Wenn die Fehlermeldung „Timeout“ erscheint, hat der Controller sich nicht ordnungsgemäß gemeldet. Überprüfen Sie in diesem Fall die Netzwerkeinstellungen.

```

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

Ping-Statistik für 192.168.1.17:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
    Ca. Zeitangaben in Millisek.:
    Minimum = 6ms, Maximum = 6ms, Mittelwert = 6ms

U:\>_
  
```

Abbildung 8: Beispiel eines Funktionstests

5. Schließen Sie die Eingabeaufforderung, wenn der Test erfolgreich war.

## 4.5 Passwörter ändern

### **i** Hinweis

#### Passwörter ändern!

Die im Auslieferungszustand eingestellten Standardpasswörter sind in dieser Betriebsanleitung dokumentiert und bieten so keinen hinreichenden Schutz.

- Ändern Sie die Passwörter entsprechend Ihren Erfordernissen.

### **i** Hinweis

#### Zulässige Zeichen für Passwörter


Passwörter dürfen nur die folgenden Zeichen enthalten:

Kleinbuchstaben (a ... z), Großbuchstaben (A ... Z), Ziffern (0 ... 9) und Sonderzeichen (! " # \$ % & ' ( ) \* +, . / : ; < = > ? @ [ ] ^ \_ ` { } | ~ -).

Zur Erhöhung der Sicherheit sollten Passwörter eine Mischung aus Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen enthalten.

Allgemein bekannte Namen, Geburtsdaten und andere leicht zu erratende Informationen sollten nicht Bestandteil von Passwörtern sein.

Ändern Sie deshalb vor der Inbetriebnahme des Controllers die Standardpasswörter!

Für die Benutzergruppe „Linux®-Benutzer“ sind Standardpasswörter vergeben und in der Tabelle  **Linux®-Benutzer** [[▶ 35](#)] aufgelistet.

Um die Passwörter über das WBM zu ändern, gehen Sie folgendermaßen vor:

1. Verbinden Sie den Controller über eine der Netzwerk-Schnittstellen (X1, X2) mit einem PC.
2. Starten Sie auf dem PC ein Webbrowserprogramm und rufen Sie das WBM des Controllers auf.
3. Melden Sie sich am Controller als Benutzer „root“, „admin“ oder „user“ mit dem Standardpasswort an.
4. Ändern Sie das Passwort für den angemeldeten Benutzer auf der WBM-Seite „Configuration of the users for the WBM“.
5. Ändern Sie so die Passwörter für alle Benutzer.

Um die Passwörter über ein Terminalprogramm zu ändern, gehen Sie folgendermaßen vor:

1. Verbinden Sie den Controller über die Netzwerkschnittstelle X1 mit einem PC.
2. Starten Sie auf dem PC ein Terminalprogramm.
3. Melden Sie sich am Controller als Benutzer „root“ mit dem Standardpasswort an.
4. Ändern Sie das Passwort für alle Benutzer mit den Befehlen „passwd root“, „passwd admin“ und „passwd user“.

## 4.6 Ausschalten/Neustart

Um den Controller auszuschalten, schalten Sie die Versorgungsspannung ab.

Um einen Software-Reset (Neustart) des Controllers durchzuführen, betätigen Sie den Reset-Taster. Alternativ schalten Sie den Controller aus und anschließend wieder ein.

### Hinweis

#### **Neustart nach Parameteränderungen nicht durch Aus- und Wiedereinschalten hervorrufen!**

Einige Parameteränderungen erfordern einen Neustart des Controllers, um wirksam zu werden. Das Speichern der Änderungen benötigt eine gewisse Zeit.

Schalten Sie den Controller nicht aus und wieder ein, um einen Neustart auszuführen, da durch ein frühzeitiges Ausschalten Änderungen verloren gehen können.

Führen Sie einen Neustart nur durch die softwaremäßige Reboot-Funktion aus. Damit ist sichergestellt, dass alle Speichervorgänge richtig und vollständig abgeschlossen sind.

# 5 Konfigurieren

## 5.1 Konfigurieren im WBM

Die HTML-Seiten (im Folgenden kurz: Seiten) des Web-Based-Managements (WBM) dienen zur Konfiguration des Controllers. Für den Zugriff auf das WBM über einen Webbrowser gehen Sie folgendermaßen vor:

1. Verbinden Sie den Controller über die ETHERNET-Schnittstelle X1 und das ETHERNET-Netzwerk oder über die USB-Service-Schnittstelle und ein USB-Service-Kabel mit Ihrem PC.
2. Starten Sie einen Webbrowser auf Ihrem PC.
3. Geben Sie in die Adresszeile Ihres Webbrowsers „https://“, gefolgt von der IP-Adresse des Controllers und „/wbm“ ein, z. B. „https://192.168.1.17/wbm“. Beachten Sie, dass sich PC und Controller im selben Subnetz befinden müssen, siehe Einstellen einer IP-Adresse.

Wenn Sie die IP-Adresse nicht kennen und nicht ermitteln können, schalten Sie den Controller temporär auf die feste voreingestellte IP-Adresse „192.168.1.17“ um, siehe Temporär feste IP-Adresse einstellen.

**Hinweis**

**Auslastung durch CODESYS-Programm berücksichtigen!**

Wenn der Controller durch ein CODESYS-Programm ausgelastet ist, kann dies zu einer verlangsamteten Verarbeitung im WBM führen. Unter Umständen werden deshalb Time-out-Fehler gemeldet.

- Stoppen Sie vor umfangreichen Konfigurationen die CODESYS Applikation über das WBM.

⇒ Wenn die Verbindung aufgebaut werden konnte, wird ein Anmeldefenster angezeigt.

## Authentication

Hostname: PFC200V3-42E739  
Application: Web-based Management

Username

Password

< cancel > Login

Abbildung 9: Anmeldefenster

4. Geben Sie den Benutzernamen und das Passwort ein.
  5. Klicken Sie auf die Schaltfläche [**> Login**].
- ➔ Abhängig vom ausgewählten Benutzer werden die Navigationsleiste und die Register des WBM angezeigt.

Sollten Sie in Ihrem Webbrowser Cookies deaktiviert haben, können Sie weiter das WBM benutzen, solange Sie sich direkt darin bewegen. Wenn Sie jedoch die Webseite einmal komplett neu laden (z. B. mit **[F5]**), müssen Sie sich neu einloggen, da der Webbrowser in diesem Fall keine Möglichkeit hat, die Daten Ihrer Login-Session abzuspeichern.

### 5.1.1 Allgemeine Seiteninformationen

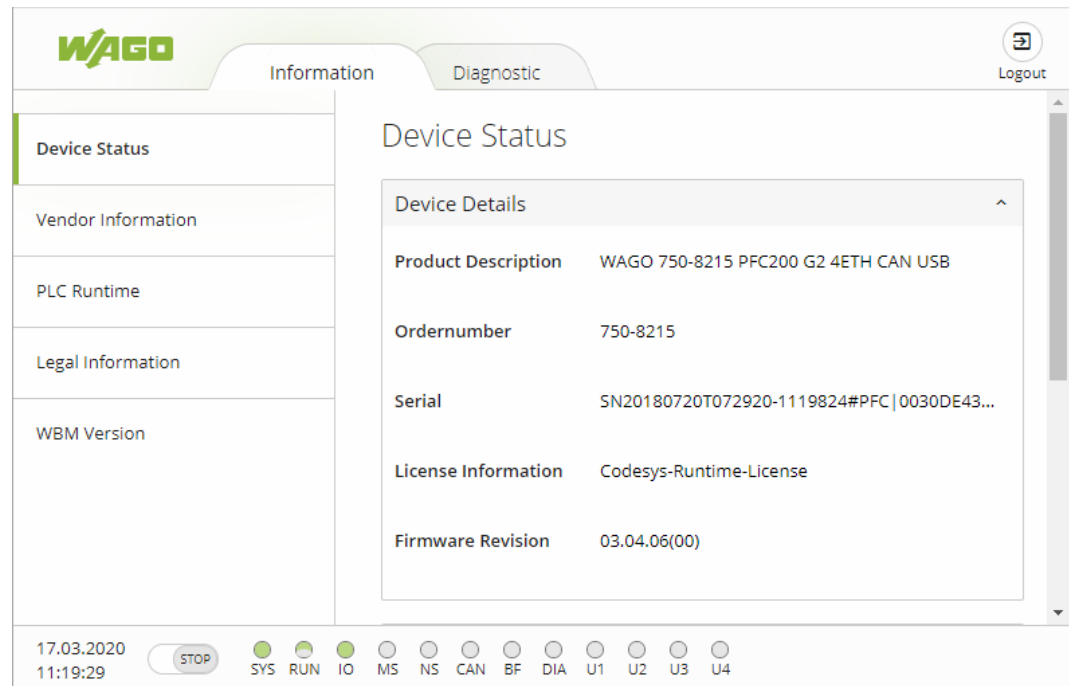


Abbildung 10: WBM-Browserfenster (Beispiel)

In der Kopfzeile des Browserfensters werden die Registerkarten für die verschiedenen WBM-Bereiche sowie die Schaltflächen **[Reboot]** und **[Logout]** angezeigt. Die Schaltfläche **[Reboot]** ist nur sichtbar, wenn Sie als Administrator angemeldet sind. Über die Schaltfläche **[Reboot]** können Sie einen Neustart des Controllers ausführen. Ein Neustart kann einige Minuten dauern. Über die Schaltfläche **[Logout]** melden Sie den aktuellen Benutzer ab, wenn Sie die Oberfläche nicht weiter verwenden möchten. Sie gelangen dann wieder zur Anmeldeaufforderung.

Wenn nicht alle Registerkarten in der gewählten Breite des Fensters darstellbar sind, wird anstelle der nicht darstellbaren Registerkarten eine Registerkarte mit Auslassungszeichen (...) angezeigt. Damit können Sie über ein Pull-down-Menü die nicht dargestellten Registerkarten auswählen.

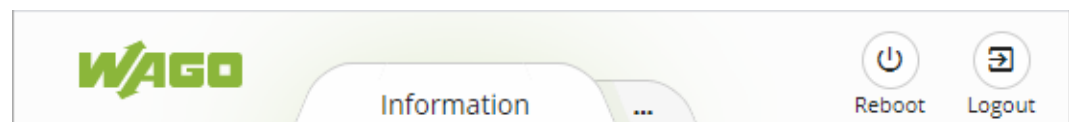


Abbildung 11: WBM-Kopfzeile mit nicht darstellbaren Registerkarten (Beispiel)

Auf der linken Seite des Browserfensters wird der Navigationsbaum angezeigt. Der Inhalt des Navigationsbaums ist abhängig von der ausgewählten Registerkarte. Über den Navigationsbaum können Sie die einzelnen Seiten und, falls vorhanden, deren Unterseiten erreichen.

In der Statuszeile wird der aktuelle Gerätezustand angezeigt.

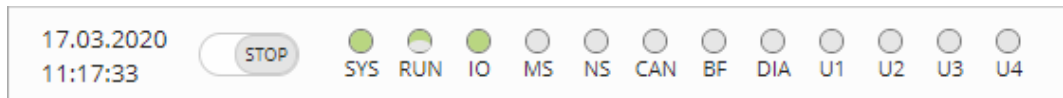


Abbildung 12: WBM-Statuszeile (Beispiel)

- Datum und Uhrzeit – lokale Zeit und lokales Datum auf dem Gerät
- Zustand des Betriebsartenschalters
- LED-Zustände des Gerätes:  
 Die LEDs sind mit ihrer jeweiligen Bezeichnung beschriftet. Die Zustände werden über eine Grafik symbolisiert. Es sind folgende Darstellungen möglich:
  - Grau: Die LED ist ausgeschaltet.
  - Vollflächige Farbe: Die LED ist in der jeweiligen Farbe eingeschaltet.
  - Halbflächige Farbe: Die LED blinkt in der entsprechenden Farbe. Die andere Hälfte der Fläche ist dann entweder grau oder ebenfalls gefärbt. Letzteres bedeutet, dass die LED sequenziell in verschiedenen Farben blinkt.
 Solange der Mauszeiger sich über einer LED befindet, öffnet sich ein Tooltip mit weiteren Informationen. Der angezeigte Text enthält die Meldung, die die LED in ihren aktuellen Zustand versetzt hat. Hier ist auch die Zeitangabe der Meldung enthalten.  
 Die im WBM angezeigten Zustände entsprechen nicht zu jedem Zeitpunkt genau denen auf dem Controller. Die Daten haben bei der Übertragung eine Laufzeit und können auch nur in einem bestimmten Intervall abgefragt werden. Die Zeitdauer zwischen zwei Abfragen beträgt 30 Sekunden.

### 5.1.2 WBM-Seitenübersicht und Zugriffsrechte

Für die WBM-Seiten sind die in der nachfolgenden Tabelle aufgeführten Zugriffsrechte erforderlich. Benutzer mit geringeren Rechten können die Seiten ggf. nicht aufrufen oder nur anzeigen.

Tabelle 120: Zugriffsrechte für die WBM-Seiten

Registerkarte	Navigation	WBM-Seitentitel	Benutzer
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	
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 Domainname	user
	Routing	Routing	user
	STP/RSTP	Spanning Tree Protocol	user
	Clock	Clock Settings	user
	Administration		
	Serial Interface	Configuration of Serial Interface RS232/RS485	admin
	Service Interface	Configuration of Service Interface	admin
	Create Image	Create bootable Image	admin

Registerkarte	Navigation	WBM-Seitentitel	Benutzer
	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 Server	admin
	Cloud Connectivity		
	Status	Status Overview	admin
	Connection <n>	Configuration of Connection <n>	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 Parameters	admin
	Commissioning		
	Commissioning Settings		
	admin		
Docker			
DockerSettings			
admin			
Users			
WBM User Configuration			
admin			
Modem			
Configuration of internal 4G Modem			
admin			
Fieldbus	OPC UA		
	OPC UA Configuration		
	admin		
	PROFIBUS DP		
	Configuration of PROFIBUS DP Slave		
	user		
	BACnet		
Status	BACnet Status	admin	
Configuration	BACnet Configuration	admin	
Data Link	BACnet Data Link	admin	
Storage Location	BACnet Storage Location	admin	
Info	BACnet Info	admin	
Security	Open VPN/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			

## 5.2 Konfigurieren mit „WAGO Ethernet Settings“

Mit dem Programm „WAGO Ethernet Settings“ haben Sie die Möglichkeit, Systeminformationen über Ihren Controller auszulesen, Netzwerkeinstellungen vorzunehmen und den Webserver zu aktivieren/deaktivieren.

### Hinweis

#### Softwareversion beachten!

Verwenden Sie zur Konfiguration des Controllers mindestens die Version 06.15.01 vom 2021-02-08 von „WAGO Ethernet Settings“.

Nach dem Starten von „WAGO Ethernet Settings“ müssen Sie die entsprechende Schnittstelle auswählen.

Zur Datenkommunikation können Sie ein geeignetes USB-C-Service-Kabel oder ggf. das IP-Netzwerk verwenden.

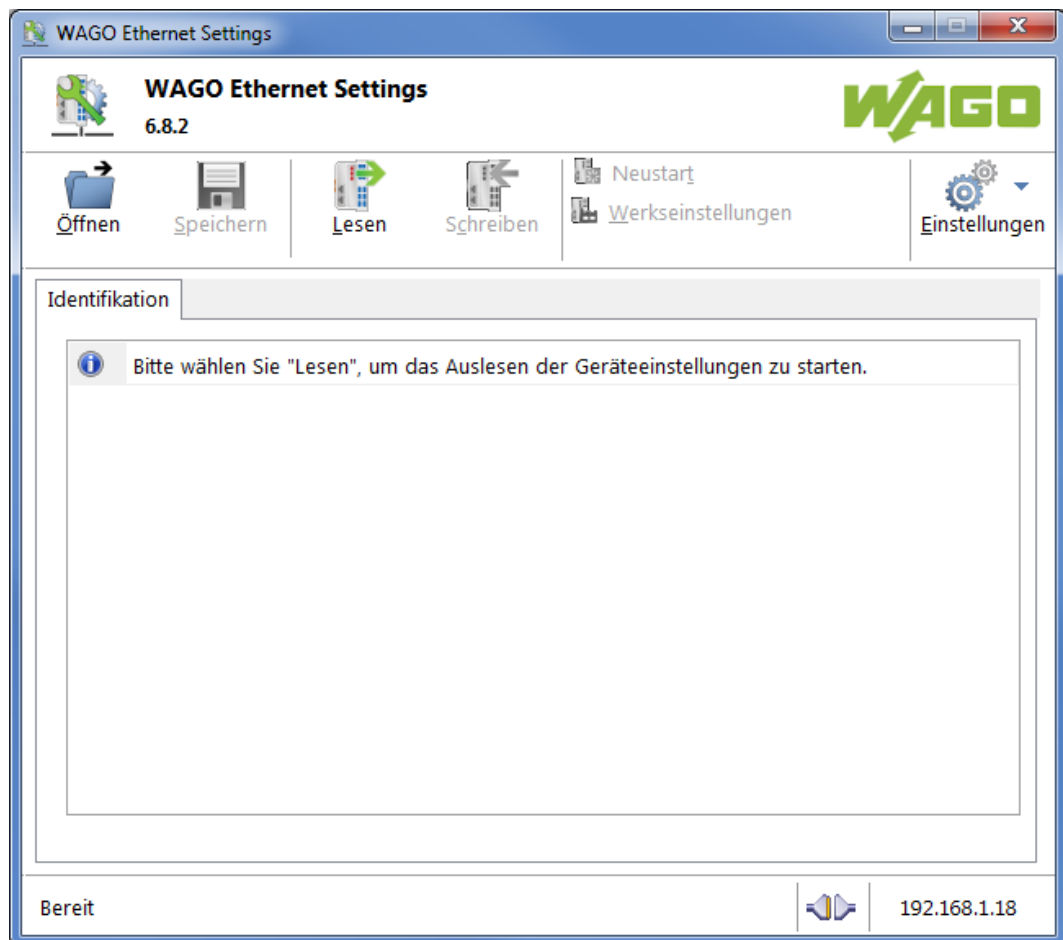


Abbildung 13: „WAGO Ethernet Settings“ – Startbildschirm (Beispiel)

- Klicken Sie hierzu auf „Einstellungen“ und dann auf „Kommunikation“.
- ➔ Im nun neu geöffneten Fenster „Kommunikationseinstellungen“ nehmen Sie die Einstellungen entsprechend Ihren Erfordernissen vor.

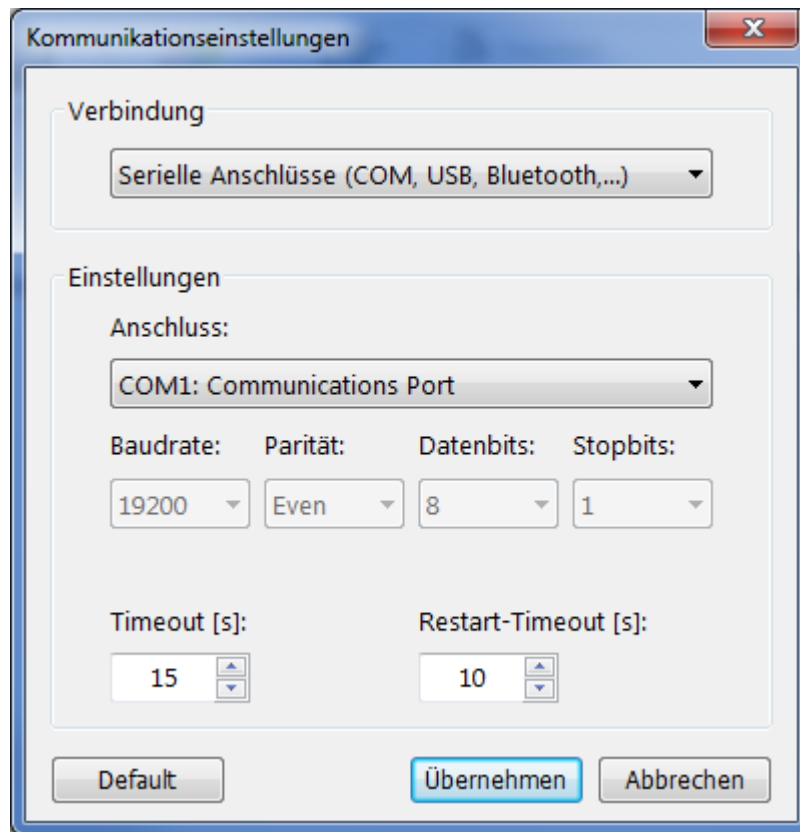


Abbildung 14: „WAGO Ethernet Settings“ – Kommunikationsverbindung (Beispiel)

Haben Sie „WAGO Ethernet Settings“ konfiguriert und auf **[Übernehmen]** geklickt, wird automatisch die Verbindung mit dem Controller aufgebaut.

Wurde „WAGO Ethernet Settings“ mit den korrekten Parametern bereits gestartet, ist es möglich, durch Klicken auf **[Lesen]** die Verbindung zum Controller aufzubauen.

### 5.2.1 Registerkarte Identifikation

Hier finden Sie einen Überblick über das angeschlossene Produkt.

Neben einigen festen Werten wie Artikelnummer, MAC-Adresse und Firmwareversion ist auch die aktuell verwendete IP-Adresse und die Art, wie sie konfiguriert wurde, ersichtlich.

Identifikation	Netzwerk	SPS	Status
Artikelnummer	750-8210		
Bezeichnung	WAGO 750-8210 PFC200 G2 4ETH		
FW Version	04.01.09(00)		
HW Version	01		
FWL Version	2021.10.0w04.00.00 IDX=14		
Seriennummer	37SUN31564010260372744+9999999999999999		
MAC-Adresse	0030DE46C828		
IP-Adresse	192.168.1.10 (Statische Konfiguration)		
Laufzeitsystem	CODESYS V3		

Abbildung 15: „WAGO Ethernet Settings“ – Registerkarte Identifikation (Beispiel)

## 5.2.2 Registerkarte Netzwerk

Dieser Reiter wird verwendet um die Netzwerkeinstellungen zu konfigurieren.

In der Spalte „Eingabe“ können Werte verändert werden und in der Spalte „Aktuell Verwendet“ sind die aktuell tatsächlich verwendeten Parameter zu sehen.

Identifikation	Netzwerk	SPS	Status																														
	<table border="1"> <thead> <tr> <th>Parameter</th> <th>Eingabe</th> <th>Aktuell verwendet</th> </tr> </thead> <tbody> <tr> <td>Bezugsquelle</td> <td>Statische Konfiguration</td> <td>Statische Konfiguration</td> </tr> <tr> <td>IP-Adresse</td> <td>192.168.1.18</td> <td><b>192.168.1.18</b></td> </tr> <tr> <td>Subnetzmaske</td> <td>255.255.255.0</td> <td>255.255.255.0</td> </tr> <tr> <td>Gateway</td> <td>0.0.0.0</td> <td>0.0.0.0</td> </tr> <tr> <td>Bevorzugter DNS-Server</td> <td>0.0.0.0</td> <td>0.0.0.0</td> </tr> <tr> <td>Alternativer DNS-Server</td> <td>0.0.0.0</td> <td>0.0.0.0</td> </tr> <tr> <td>Zeit-Server</td> <td>0.0.0.0</td> <td>0.0.0.0</td> </tr> <tr> <td>Host-Name</td> <td></td> <td>PFC200-400E6F</td> </tr> <tr> <td>Domain-Name</td> <td>localdomain.lan</td> <td>localdomain.lan</td> </tr> </tbody> </table>	Parameter	Eingabe	Aktuell verwendet	Bezugsquelle	Statische Konfiguration	Statische Konfiguration	IP-Adresse	192.168.1.18	<b>192.168.1.18</b>	Subnetzmaske	255.255.255.0	255.255.255.0	Gateway	0.0.0.0	0.0.0.0	Bevorzugter DNS-Server	0.0.0.0	0.0.0.0	Alternativer DNS-Server	0.0.0.0	0.0.0.0	Zeit-Server	0.0.0.0	0.0.0.0	Host-Name		PFC200-400E6F	Domain-Name	localdomain.lan	localdomain.lan		<div style="border: 1px solid gray; padding: 5px;"> <p>Schnittstelle X1</p> <p>Schnittstelle X2</p> <p>Starte <u>W</u>BM</p> <hr/> <p>Schnittstellen</p> <p><input type="radio"/> als Switch</p> <p><input checked="" type="radio"/> getrennt</p> </div>
Parameter	Eingabe	Aktuell verwendet																															
Bezugsquelle	Statische Konfiguration	Statische Konfiguration																															
IP-Adresse	192.168.1.18	<b>192.168.1.18</b>																															
Subnetzmaske	255.255.255.0	255.255.255.0																															
Gateway	0.0.0.0	0.0.0.0																															
Bevorzugter DNS-Server	0.0.0.0	0.0.0.0																															
Alternativer DNS-Server	0.0.0.0	0.0.0.0																															
Zeit-Server	0.0.0.0	0.0.0.0																															
Host-Name		PFC200-400E6F																															
Domain-Name	localdomain.lan	localdomain.lan																															

Abbildung 16: „WAGO Ethernet Settings“ – Registerkarte Netzwerk (Beispiel)

### Bezugsquelle

Wählen Sie hier aus, wie der Controller seine IP-Adresse ermitteln soll: Statisch, per DHCP oder per BootP.

### IP-Adresse, Subnetzmaske, Gateway

Geben Sie hier im Falle der statischen Konfiguration die jeweiligen Netzwerkparameter ein.

**i Hinweis****Eingeschränkte Einstellung für Default-Gateways!**

Mit „WAGO Ethernet Settings“ kann nur das Default-Gateway 1 eingestellt werden. Das Default-Gateway 2 kann ausschließlich im WBM eingestellt werden!

**Bevorzugter DNS-Server, Alternativer DNS-Server**

Geben Sie hier bei Bedarf die IP-Adresse eines erreichbaren DNS Servers für die Auflösung von Netzwerknamen ein.

**Zeit-Server**

Geben Sie hier die IP-Adresse eines Zeitservers ein, wenn der Controller seine Systemzeit über NTP einstellen soll.

**Host-Name**

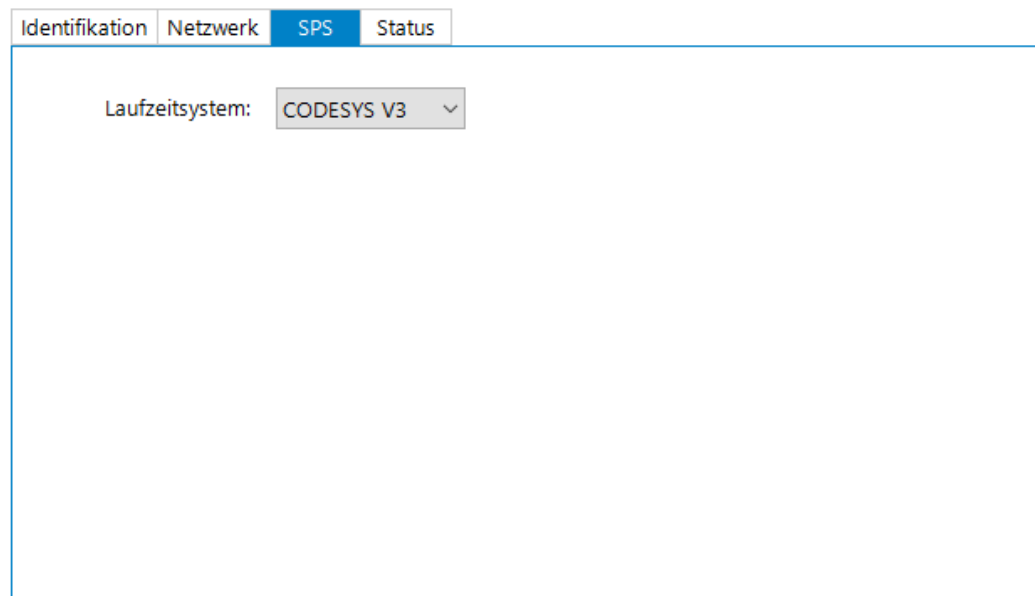
Hier wird der Hostname des Controllers angezeigt. Im Auslieferungszustand wird der Hostname zusammengesetzt aus dem String „PFCx00-“ und den letzten 3 Byte der MAC-Adresse. Dieser Standardwert wird ebenfalls immer dann verwendet, wenn der selbstgewählte Name in der Spalte „Eingabe“ gelöscht wird.

**Domain-Name**

Hier wird der aktuelle Domain-Name angezeigt. Diese Einstellung kann bei dynamischen Konfigurationen z. B. DHCP automatisch überschrieben werden.

**5.2.3 Registerkarte SPS**

Hier können Sie das Laufzeitsystem auswählen.



The screenshot shows a web interface with four tabs: 'Identifikation', 'Netzwerk', 'SPS', and 'Status'. The 'SPS' tab is active and highlighted in blue. Below the tabs, there is a label 'Laufzeitsystem:' followed by a dropdown menu. The dropdown menu is currently set to 'CODESYS V3' and has a small downward arrow on the right side.

Abbildung 17: „WAGO Ethernet Settings“ – Registerkarte Protokoll (Beispiel)

**5.2.4 Registerkarte Status**

Hier werden allgemeine Informationen über den Status des Controllers angezeigt.

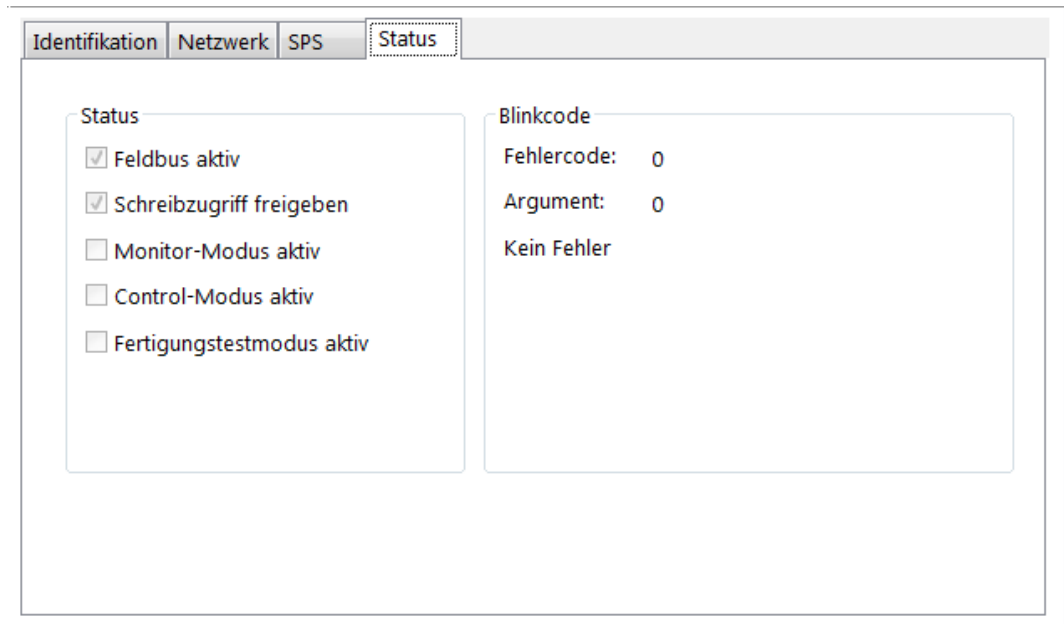


Abbildung 18: „WAGO Ethernet Settings“ – Registerkarte Status (Beispiel)

# 6 Service

## 6.1 Firmwareänderungen

### ⚠ ACHTUNG

#### Controller nicht ausschalten!

Durch eine Unterbrechung des Update-/Downgrade-Vorgangs kann der Controller beschädigt werden.

- Schalten Sie den Controller während des Update-/Downgrade-Vorgangs nicht aus und unterbrechen Sie nicht die Spannungsversorgung!

### ℹ Hinweis

#### Firmwareversion beachten!

Bei Geräten mit einer werksseitigen Installation einer Firmware  $\geq$  FW 05 ist ein einfaches Downgrade auf eine Version  $\leq$  FW 04 nicht möglich!

Verwenden Sie ein spezielles Downgrade-Image.

### ℹ Hinweis

#### Zur Firmwarezielversion passende Dokumentation bereithalten!

Durch eine Firmwareänderung können Eigenschaften und Funktionen des Controllers verändert, entfernt oder hinzugefügt werden. Damit können ggf. in dieser Dokumentation beschriebene Eigenschaften und Funktionen nicht zur Verfügung stehen oder Eigenschaften oder Funktionen des Controllers in dieser Dokumentation nicht beschrieben sein.

1. Verwenden Sie daher nach einer Firmwareänderung nur die zur Zielfirmware passende Dokumentation.
2. Bei Rückfragen wenden Sie sich an den WAGO Support.

Sie können die Firmware auf zwei verschiedene Arten aktualisieren:

- mit WAGOupload
- mit Speicherkarte und WBM

### 6.1.1 Firmware-Update/-Downgrade mit WAGOupload durchführen

1. Starten Sie WAGOupload.
2. Klicken Sie auf die Tätigkeit **[Firmware aktualisieren]**.
3. Geben Sie im Dialogfenster „Zielcontroller wählen“ bei der Option „Übertragung über TCP/IP“ die IP-Adresse Ihres Controllers ein.
4. Klicken Sie auf **[Controller suchen]**.
  - ⇒ In der Liste wird nun Ihr Controller angezeigt.
5. Markieren Sie den angezeigten Controller und klicken Sie auf **[Weiter]**.

6. Wählen Sie im Dialogfenster „Update-Datei wählen“ die \*.wup-Firmwaredatei zur gewünschten Firmware aus.
  7. Klicken Sie auf **[Weiter]**.
  8. Bestätigen Sie die Zusammenfassung mit **[Weiter]**
  9. Warten Sie, bis der Vorgang mit einer Statusmeldung beendet wird, und klicken Sie erst dann auf **[Beenden]**, um das Fenster zu schließen.
- ➔ Auf Ihrem Controller steht nun die neu installierte Firmware zur Verfügung.

### 6.1.2 Firmware-Update/-Downgrade mit Speicherkarte und WBM durchführen

1. Kopieren Sie zunächst die Firmware-Image-Datei der benötigten Firmware (\*.img) mit einem geeigneten PC-Tool auf die Speicherkarte.
2. Sichern Sie Ihre Anwendung und die Einstellungen des Controllers.
3. Schalten Sie den Controller aus.
4. Stecken Sie die Speicherkarte mit dem zu installierenden Firmware-Image in den Speicherkartensteckplatz.
5. Schalten Sie den Controller ein.
  - ⇒ Der Controller wird mit dem zu installierenden Firmware-Image von der Speicherkarte gestartet.
6. Öffnen Sie nach dem Hochlauf des Controllers die WBM-Seite „Administration“ > „Create Boot Image“ (ggf. müssen Sie dazu die IP-Adresse temporär ändern).
7. Erstellen Sie ein neues Boot-Image auf dem internen Speicher. Klicken Sie dazu die Schaltfläche **[Start Copy]**.
8. Schalten Sie nach dem Abschluss des Vorgangs den Controller aus.
9. Entfernen Sie die Speicherkarte.
10. Schalten Sie den Controller wieder ein.
  - ➔ Der Controller wird jetzt mit der neu installierten Firmware-Version vom internen Speicher gestartet.

## 6.2 Reset-Funktionen auslösen

Mit dem Betriebsartenschalter und dem Reset-Taster können Sie verschiedene Reset-Funktionen auslösen.

### 6.2.1 Warmstart-Reset

Bei einem Warmstart-Reset werden alle CODESYS V3-Applikationen zurückgesetzt. Alle globalen Daten werden auf ihre Initialisierungswerte gesetzt. Dies entspricht dem CODESYS V3-IDE-Befehl „Reset warm“.

- Um einen Warmstart-Reset durchzuführen, bringen Sie den Betriebsartenschalter in die Reset-Position und halten ihn dort länger als 2 Sekunden aber kürzer als 7 Sekunden.
- ➔ Die Ausführung wird durch ein kurzes Erlöschen der roten „RUN“-LED nach dem Loslassen des Betriebsartenschalters signalisiert.

### 6.2.2 Kaltstart-Reset

Bei einem Kaltstart-Reset werden alle CODESYS V3-Applikationen zurückgesetzt. Alle globalen Daten und die Retain-Variablen werden auf ihre Initialisierungswerte gesetzt. Dies entspricht dem CODESYS V3-IDE-Befehl „Reset kalt“.

1. Um einen Kaltstart-Reset durchzuführen, bringen Sie den Betriebsartenschalter in die Reset-Position und halten Sie ihn dort länger als 7 Sekunden.
  - ⇒ Die Ausführung wird nach Ablauf der 7 Sekunden durch ein längeres Erlöschen der roten „RUN“-LED signalisiert.
2. Lassen Sie den Betriebsartenschalter anschließend wieder los.

### 6.2.3 Software-Reset (Neustart)

Bei einem Software-Reset wird das Produkt neu gestartet.

- Um einen Software-Reset durchzuführen, bringen Sie den Betriebsartenschalter in die „RUN“- oder „STOP“-Position und betätigen Sie den Reset-Taster länger als 1 Sekunde aber kürzer als 8 Sekunden.
- ➔ Die Ausführung wird durch ein kurzes Aufleuchten aller LEDs signalisiert. Nach einigen weiteren Sekunden signalisiert die „SYS“-LED den erfolgreichen Bootvorgang des Controllers.

### 6.2.4 Controller-Reset

#### ⚠ ACHTUNG

##### Controller nicht ausschalten!

Durch eine Unterbrechung des Reset-Vorgangs kann der Controller beschädigt werden.

- Schalten Sie den Controller während des Reset-Vorgangs nicht aus und unterbrechen Sie nicht die Spannungsversorgung!

#### ℹ Hinweis

##### Alle Parameter und Passwörter werden überschrieben!

Mit dem Reset werden alle Parameter und Passwörter überschrieben.

Gespeicherte Boot-Projekte einschließlich vorhandener Webvisualisierungsdaten werden gelöscht.

Nachinstallierte Firmwarefunktionen werden nicht überschrieben.

Softwarelizenzen bleiben erhalten.

- Bei Rückfragen wenden Sie sich an den WAGO Support.

Um einen „Controller-Reset“ durchzuführen, gehen Sie wie folgt vor:

1. Betätigen Sie den Reset-Taster und halten Sie ihn gedrückt.
2. Schieben Sie den Betriebsartenschalter in die Position „RESET“ und halten Sie ihn in dieser Position.
3. Halten Sie beide Taster, bis nach ca. 8 Sekunden die „SYS“-LED im Wechsel rot/grün blinkt.

4. Wenn die „SYS“-LED im Wechsel rot/grün blinkt, lassen Sie den Betriebsartenschalter und den Reset-Taster los.  
➔ Der Controller wurde zurückgesetzt und führt einen automatischen Neustart aus.

### **i Hinweis**

#### **Reset-Vorgang nicht unterbrechen!**

Wenn Sie den Reset-Taster zu früh loslassen, dann startet das Produkt neu, ohne den Controller-Reset durchzuführen.

## **6.3 Root-Zertifikate aktualisieren**

Wenn Sie die Root-Zertifikate auf dem Controller aktualisieren möchten, gehen Sie folgendermaßen vor:

1. Laden Sie das aktuelle Root-CA-Bundle von der Webseite <https://curl.haxx.se/ca> auf Ihren PC herunter.
2. Benennen Sie die Datei um nach „ca-certificates.crt“.
3. Übertragen Sie die Datei mit einem SFTP- oder FTP-Client auf den Controller in das Verzeichnis /etc/ssl/certs.
4. Starten Sie den Controller neu. Nutzen Sie dazu die Reboot-Funktion im WBM.

# 7 Anhang

## 7.1 Konfigurationsdialoge

### 7.1.1 WBM-Seiten

#### 7.1.1.1 WBM-Seitenübersicht und Zugriffsrechte

Für die WBM-Seiten sind die in der nachfolgenden Tabelle aufgeführten Zugriffsrechte erforderlich. Benutzer mit geringeren Rechten können die Seiten ggf. nicht aufrufen oder nur anzeigen.

Tabelle 121: Zugriffsrechte für die WBM-Seiten

Registerkarte	Navigation	WBM-Seitentitel	Benutzer	
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	
		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 Domainname	user
		Routing	Routing	user
		STP/RSTP	Spanning Tree Protocol	user
		Clock	Clock Settings	user
Administration				
		Serial Interface	Configuration of Serial Interface RS232/RS485	admin
		Service Interface	Configuration of Service Interface	admin
		Create Image	Create bootable Image	admin
Package Server				
		Firmware Backup	Firmware Backup	admin
		Firmware Restore	Firmware Restore	admin
		Active System	Active System	admin
		Mass Storage	Mass Storage	admin
		Software Uploads	Software Uploads	admin
Ports and Services				
		Network Services	Configuration of Network Services	admin
		NTP Client	Configuration of NTP Client	admin
		PLC Runtime Services	PLC Runtime Services	admin
		SSH	SSH Server Settings	admin

Registerkarte	Navigation	WBM-Seitentitel	Benutzer	
	DHCP Server	DHCP Server Configuration	admin	
	DNS	Configuration of DNS Server	admin	
	Cloud Connectivity			
	Status	Status Overview	admin	
	Connection <n>	Configuration of Connection <n>	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 Parameters	admin	
	Commissioning	Commissioning Settings	admin	
	Docker	DockerSettings	admin	
	Users	WBM User Configuration	admin	
	Modem	Configuration of internal 4G Modem	admin	
	Fieldbus	OPC UA	OPC UA Configuration	admin
PROFIBUS DP		Configuration of PROFIBUS DP Slave	user	
BACnet				
Status		BACnet Status	admin	
Configuration		BACnet Configuration	admin	
Data Link		BACnet Data Link	admin	
Storage Location		BACnet Storage Location	admin	
Security	Open VPN/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	

In den folgenden Abschnitten finden Sie die Beschreibung der Parameter und Einstellmöglichkeiten für die Seiten des Web-Based-Managements (WBM).

### 7.1.1.2 Registerkarte „Information“

#### 7.1.1.2.1 Seite „Device Status“

Auf der Seite „Device Status“ werden die Angaben zur Produktidentifikation und die wichtigsten Netzwerkeigenschaften angezeigt.

### Gruppe „Device Details“

In dieser Gruppe werden die Eigenschaften des Produktes angezeigt.

Tabelle 122: WBM-Seite „Device Status“ – Gruppe „Device Details“

Parameter	Bedeutung
Product Description	Bezeichnung des Produktes
Ordernumber	Bestellnummer des Produktes
Unique Item Identifier (UII)	Eindeutige Identifikationsnummer des Produktes
License Information	Anzeige, dass das Laufzeitsystem CODESYS vorhanden ist
Firmware Revision	Firmwarestand

### Gruppe „Network TCP/IP Details“

In dieser Gruppe werden die Netzwerk- und Schnittstelleneigenschaften des Produktes angezeigt.

Tabelle 123: WBM-Seite „Device Status“ – Gruppe „Network TCP/IP Details“

Parameter	Bedeutung	
DIP Switch Status	Status des Adresswahlschalters; dieser Bereich ist nur sichtbar, wenn ein Adresswahlschalter vorhanden ist.	
DIP Switch Mode	Einstellung des Adresswahlschalters	
	Off (0)	IP-Adressvergabe über z. B. WBM
	static (1 ... 254)	Statische IP-Adressvergabe über Adresswahlschalter
	dhcp (255)	Dynamische IP-Adressvergabe über DHCP
DIP Switch Value	Eingestellter Wert des Adresswahlschalters	
Interface <n>	Aktuell konfiguriertes Interface; Für jedes konfigurierte Interface werden die Eigenschaften in einem separaten Bereich dargestellt.	
Mac Address	MAC-Adresse, die zur Identifikation und Adressierung des Produktes dient	
IP Source	Aktuelle Bezugsart der IP-Adresse	
	none	Es ist keine IP-Vergabemethode ausgewählt; Dies tritt z. B. auf, wenn durch Änderungen an der Bridge-Konfiguration eine Bridge hinzugefügt wurde. Wählen Sie im Register <b>Configuration</b> auf der Seite <b>TCP/IP Configuration</b> eine Bezugsquelle aus.
	static IP	Statische IP-Adressvergabe
	dhcp	Dynamische IP-Adressvergabe über DHCP
	bootp	Dynamische IP-Adressvergabe über BootP
	external	Die IP-Adresse wird ggf. durch die Feldbusapplikation vergeben; Dies tritt z. B. auf, wenn die IP-Adresse durch die Applikation gesteuert wird.
IP Address	Aktuelle IP-Adresse des Produktes	
Subnet Mask	Aktuelle Subnetzmaske des Produktes	

#### 7.1.1.2.2 Seite „Vendor Information“

Auf der Seite „Vendor Information“ finden Sie Hersteller und Anschrift.

### 7.1.1.2.3 Seite „PLC Runtime Information“

Auf der Seite „PLC Runtime Information“ finden Sie Informationen zu dem aktivierten Laufzeitsystem.

Außerdem finden Sie hier einen Link, um die WebVisu zu öffnen.

#### Gruppe „Runtime“

Tabelle 124: WBM-Seite „PLC Runtime Information“ – Gruppe „Runtime“

Parameter	Bedeutung
Version	Aktuell aktiviertes Laufzeitsystem Bei ausgeschaltetem Laufzeitsystem wird „None“ angezeigt.

#### Gruppe „WebVisu“

Hier finden Sie einen Link, über den Sie die WebVisu öffnen können.

### 7.1.1.2.4 Seite „WAGO Software License Agreement“

Auf der Seite „WAGO Software License Agreement“ werden die Lizenzbedingungen für die im Produkt eingesetzte Software von WAGO aufgelistet.

### 7.1.1.2.5 Seite „Open Source Licenses“

Auf der Seite „Open Source Licenses“ werden die Lizenzbedingungen für die im Produkt eingesetzte Open-Source-Software in alphabetischer Reihenfolge aufgelistet.

### 7.1.1.2.6 Seite „WBM Third Party License Information“

Auf der Seite „WBM Third Party License Information“ finden Sie die Lizenztexte der Open-Source-Lizenzen, die das WBM selber betreffen.

### 7.1.1.2.7 Seite „Trademarks Information“

Auf der Seite „Trademarks Information“ finden Sie eine Auflistung der Schutz- und Markenrechte.

### 7.1.1.2.8 Seite „WBM Version“

Auf der Seite „WBM Version“ finden Sie die Versionsinformationen über die verschiedenen Bereiche („Plugins“), die im WBM enthalten sind. Diese Informationen sind eventuell nützlich für den Support, wenn ein Fehler im WBM festgestellt wird.

## 7.1.1.3 Registerkarte „Configuration“

### 7.1.1.3.1 Seite „PLC Runtime Configuration“

Auf der Seite „PLC Runtime Configuration“ finden Sie die Einstellungen zu dem mit der Programmiersoftware erstellten Boot-Projekt und die Einstellungen zu der im Laufzeitsystem erstellten Webvisualisierung.

### Gruppe „General PLC Runtime Configuration“

Die Änderung des Laufzeitsystems wird sofort wirksam.

Die Änderung des Home-Verzeichnisses wird erst nach dem nächsten Neustart des Produktes wirksam. Nutzen Sie hierzu die Reboot-Funktion des WBM. Schalten Sie das Produkt nicht zu früh aus.

Tabelle 125: WBM-Seite „PLC Runtime Configuration“ – Gruppe „General PLC Runtime Configuration“

Parameter	Bedeutung	
PLC Runtime Version	Auswahl des aktiven SPS-Laufzeitsystems	
	none	Es ist kein Laufzeitsystem aktiviert.
	CODESYS V3	Das Laufzeitsystem CODESYS V3 ist aktiviert.
Home directory on memory card enabled	Auswahl des Speicherortes für das Home-Verzeichnis des Laufzeitsystems	
	<input type="checkbox"/>	Das Home-Verzeichnis wird im internen Speicher abgelegt.
	<input checked="" type="checkbox"/>	Das Home-Verzeichnis wird auf die Speicherkarte ausgelagert.
[Submit]	Änderung übernehmen	

#### Hinweis

##### Löschen aller Daten bei Umschaltung des Laufzeitsystems

Bei der Umschaltung des Laufzeitsystems wird das Home-Verzeichnis für das Laufzeitsystem komplett gelöscht.

#### Hinweis

##### Vor Umschaltung des Home-Verzeichnisses Speicherkarte einstecken!

Nur die erste Partition einer Speicherkarte ist unter /media/sd erreichbar und kann als Home-Verzeichnis benutzt werden.

- Wenn das Home-Verzeichnis auf die Speicherkarte ausgelagert werden soll, müssen Sie eine mit einem unterstützten File-System formatierte Speicherkarte einstecken.

### Gruppe „Webserver Configuration“

Die Änderung wird sofort wirksam.

Tabelle 126: WBM-Seite „PLC Runtime Configuration“ – Gruppe „Webserver Configuration“

Parameter	Bedeutung	
CODESYS 3 Webserver State	Status (enabled/disabled) des CODESYS V3-Webservers	
Default Webserver	Auswahl der Seitenanzeige bei alleiniger Eingabe der IP-Adresse des Produktes	
	Web-Based- Management	Das Web-Based-Management wird angezeigt.
	WebVisu	Die Webvisualisierung des Laufzeitsystems wird angezeigt.
[Submit]	Änderung übernehmen	

Im Auslieferungszustand wird bei alleiniger Eingabe der IP-Adresse das WBM aufgerufen.

Zur Aktualisierung der Anzeige nach einer Umschaltung geben Sie die IP-Adresse in der Adresszeile des Webbrowsers neu ein.

Voraussetzung für die Anzeige der Webvisualisierung ist ein eingeschalteter Webserver (im WBM unter „Ports and Services“ > „PLC Runtime Services“) und das Vorhandensein einer entsprechend konfigurierten Applikation.

Unabhängig von der Einstellung des Default-Webserver kann jederzeit das WBM mit „https://<IP-Adresse>/wbm“ und die Webvisualisierung mit „https://<IP-Adresse>/webvisu“ aufgerufen werden.

### **i Hinweis**

#### **Mögliche Fehlermeldungen beim Aufruf der Webvisualisierung**

Die Anzeige „500 - Internal Server Error“ weist auf einen nicht eingeschalteten Webserver hin.

Eine Seite mit der Überschrift „WebVisu not available“ weist darauf hin, dass keine Applikation mit Webvisualisierung in das Produkt geladen wurde.

#### **7.1.1.3.2 Seite „TCP/IP Configuration“**

Auf der Seite „TCP/IP Configuration“ finden Sie die TCP/IP-Einstellungen zu den ETHERNET-Schnittstellen.

##### **Gruppe „Bridge Interfaces“**

Für jede konfigurierte Bridge werden die Eigenschaften in einem separaten Bereich dargestellt.

Tabelle 127: WBM-Seite „TCP/IP Configuration“ – Gruppe „Bridge Interfaces“

Parameter	Bedeutung	
Bridge <n>	Einstellungen für die ausgewählte Bridge	
Current IP Address	Aktuelle IP-Adresse	
Current Subnet Mask	Aktuelle Subnetzmaske	
Current Default Gateway	IP-Adresse des aktuellen Default-Gateways	
IP Source	IP-Adressierung auswählen.	
	Static IP	Statische IP-Adressierung
	DHCP	Dynamische IP-Adressierung über DHCP
	BootP	Dynamische IP-Adressierung über BootP
Static IP Address	Statische IP-Adresse eingeben; die IP-Adresse ist aktiv, wenn im Auswahlfeld <b>IP Source</b> „Static IP“ aktiviert ist.	
Subnet Mask	Subnetzmaske eingeben; die Subnetzmaske ist aktiv, wenn im Auswahlfeld <b>IP Source</b> „Static IP“ aktiviert ist.	
Default Gateway	IP-Adresse des Default-Gateways eingeben	
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.	

##### **Gruppe „Dummy Interfaces“**

Für jedes konfigurierte Dummy-Interface werden die Eigenschaften in einem separaten Bereich dargestellt.

Tabelle 128: WBM-Seite „TCP/IP Configuration“ – Gruppe „Dummy Interfaces“

Parameter	Bedeutung
Dummy <n>	Einstellungen für das ausgewählte Dummy-Interface

Parameter	Bedeutung
Current IP Address	Aktuelle IP-Adresse
Current Subnet Mask	Aktuelle Subnetzmaske
IP Source	IP-Adressierung auswählen.
	Static IP                      Statische IP-Adressierung
Static IP Address	Statische IP-Adresse eingeben; die IP-Adresse ist aktiv, wenn im Auswahlfeld <b>IP Source</b> „Static IP“ aktiviert ist.
Subnet Mask	Subnetzmaske eingeben; die Subnetzmaske ist aktiv, wenn im Auswahlfeld <b>IP Source</b> „Static IP“ aktiviert ist.
<b>[Submit]</b>	Änderung übernehmen; Die Änderung wird sofort wirksam.

### Gruppe „VLAN Interfaces“

Für jedes konfigurierte VLAN-Interface werden die Eigenschaften in einem separaten Bereich dargestellt.

Tabelle 129: WBM-Seite „TCP/IP Configuration“ – Gruppe „VLAN Interfaces“

Parameter	Bedeutung
VLAN <n>	Einstellungen für das ausgewählte VLAN-Interface
Current IP Address	Aktuelle IP-Adresse
Current Subnet Mask	Aktuelle Subnetzmaske
IP Source	IP-Adressierung auswählen.
	Static IP                      Statische IP-Adressierung
	DHCP                              Dynamische IP-Adressierung
Static IP Address	Statische IP-Adresse eingeben; die IP-Adresse ist aktiv, wenn im Auswahlfeld <b>IP Source</b> „Static IP“ aktiviert ist.
Subnet Mask	Subnetzmaske eingeben; die Subnetzmaske ist aktiv, wenn im Auswahlfeld <b>IP Source</b> „Static IP“ aktiviert ist.
<b>[Submit]</b>	Änderung übernehmen; Die Änderung wird sofort wirksam.

### Gruppe „DNS Server“

Tabelle 130: WBM-Seite „TCP/IP Configuration“ – Gruppe „DNS Server“

Parameter	Bedeutung
Active	Aktive DNS-Server; Der Index spiegelt die Anfrage-Reihenfolge wider.
Assigned by DHCP	Durch DHCP (oder BootP) zugewiesene DNS-Server; Wenn kein DNS-Server durch DHCP (oder BootP) zugewiesen wurde, wird „no DNS Servers assigned by DHCP“ angezeigt.
Assigned by user	Adressen der vom Benutzer eingetragenen DNS-Server; Wenn kein Server eingetragen wurde, erscheint die Anzeige „no DNS Servers configured“.
<b>[Delete]</b>	Ausgewählten Eintrag löschen; Die Schaltfläche ist nur sichtbar, wenn Einträge vorhanden sind.
New Server IP	Weitere DNS-Serveradressen eingeben; Es sind maximal 3 Adressen möglich.
<b>[Add]</b>	Neuen Eintrag hinzufügen.

### 7.1.1.3.3 Seite „Ethernet Configuration“

Auf der Seite „Ethernet Configuration“ finden Sie die Einstellungen zu ETHERNET.

#### Gruppe „Bridge Configuration“

Tabelle 131: WBM-Seite „Ethernet Configuration“ – Gruppe „Bridge Configuration“

Parameter	Bedeutung
Bridge 1 ... <n>	Zuordnung der physikalischen Ports X1 ... X<n> zu einer logischen Bridge; Klicken Sie dazu die entsprechende Optionsschaltfläche. Die Zuordnung wird farblich markiert. Ein Port kann immer nur einer Bridge zugeordnet werden.
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.

#### Gruppe „Dummy Interfaces“

Tabelle 132: WBM-Seite „Ethernet Configuration“ – Gruppe „Dummy Interfaces“

Parameter	Bedeutung
Name	Name des ausgewählten Dummy-Interfaces
[Delete]	Ausgewählten Eintrag löschen; Die Schaltfläche ist nur sichtbar, wenn Einträge vorhanden sind.
Add Dummy Interface	Neues Dummy-Interface anlegen
Name	Namen des neuen Dummy-Interfaces eingeben
[Add]	Neuen Eintrag hinzufügen.

#### Gruppe „VLAN Interfaces“

Tabelle 133: WBM-Seite „Ethernet Configuration“ – Gruppe „VLAN Interfaces“

Parameter	Bedeutung
Name	Name des ausgewählten VLAN-Interfaces
VLAN-ID	VLAN-ID des ausgewählten VLAN-Interfaces
Link	Zugeordnete Bridge des ausgewählten VLAN-Interfaces
[Delete]	Ausgewählten Eintrag löschen; Die Schaltfläche ist nur sichtbar, wenn Einträge vorhanden sind.
Add VLAN Interface	Neues VLAN-Interface anlegen
Name	Namen des neuen VLAN-Interfaces eingeben
VLAN-ID	VLAN-ID eingeben; Zulässige Werte sind 3 ... 4094.
Link	Zugeordnete Bridge auswählen
[Add]	Neuen Eintrag hinzufügen.

#### Gruppe „Port Mirror Settings“

##### PFC100 G2, PFC200 G2 - 2-Port, PFC300

Tabelle 134: WBM-Seite „Ethernet Configuration“ – Gruppe „Port Mirror Settings“

Parameter	Bedeutung
Enabled	Spiegelung des Datenverkehrs zwischen den Ports ein-/ausschalten. <input type="checkbox"/> Datenverkehr wird nicht gespiegelt (Werkseinstellung). <input checked="" type="checkbox"/> Datenverkehr wird zwischen den ausgewählten Ports gespiegelt.
Source	Quellport des gespiegelten Datenverkehrs (X1 ... X<n>)
Destination	Zielpport des gespiegelten Datenverkehrs (X1 ... X<n>)

Parameter	Bedeutung
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.

**Die Gruppe „Port Mirror “ ist nicht bei PFC200 G2 - 4-Port-Produkten vorhanden.**

### Gruppe „Strom Control Settings“

#### PFC100 G2, PFC200 G2 - 2-Port

Tabelle 135: WBM-Seite „Ethernet Configuration“ – Gruppe „Storm Control Settings“

Parameter	Bedeutung
Broadcast Protection	Grenzwert der Datenpakete für Broadcast; Defaultwert: 1 % der maximalen Datenrate
Multicast Protection	Einstellung, ob die Begrenzung der Datenpakete nur für Broadcast oder für Broadcast und Multicast gemeinsam gilt
	<input type="checkbox"/> Begrenzung der Datenpakete gilt nur für Broadcast-Pakete.
	<input checked="" type="checkbox"/> Begrenzung der Datenpakete gilt für Broadcast- und Multicast-Pakete gemeinsam.
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.

#### PFC200 G2 - 4-Port

Tabelle 136: WBM-Seite „Ethernet Configuration“ – Gruppe „Storm Control Settings“

Parameter	Bedeutung
Broadcast Protection	Grenzwert der Datenpakete für Broadcast; Defaultwert: 1 Mbits
Multicast Protection	Grenzwert der Datenpakete für Multicast; Defaultwert: 1 Mbits

#### PFC300

Tabelle 137: WBM-Seite „Ethernet Configuration“ – Gruppe „Storm Control Settings“

Parameter	Bedeutung
Broadcast Protection	Grenzwert der Datenpakete für Broadcast; Defaultwert: 20000 Pakete pro Sekunde
Multicast Protection	Grenzwert der Datenpakete für Multicast; Defaultwert: 20000 Pakete pro Sekunde
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.

### Gruppe „Ethernet Interface Configuration“

#### PFC100 G2, PFC200 G2 - 2-Port

Tabelle 138: WBM-Seite „Ethernet Configuration“ – Gruppen „Ethernet Interface Configuration“

Parameter	Bedeutung
Interface X<n>	Für jedes im Controller vorhandenes Interface wird ein eigener Bereich angezeigt.
Enabled	Interface aktivieren/deaktivieren.
	<input type="checkbox"/> Das Interface ist deaktiviert.
	<input checked="" type="checkbox"/> Das Interface ist aktiviert.

Parameter	Bedeutung	
MAC Learning	„MAC Learning“-Funktionalität für das Interface aktivieren/deaktivieren.	
	<input type="checkbox"/>	Die „MAC Learning“-Funktionalität ist deaktiviert.
	<input checked="" type="checkbox"/>	Die „MAC Learning“-Funktionalität ist aktiviert.
Broadcast Protection Enabled	Broadcast-Protection aktivieren/deaktivieren.	
	<input type="checkbox"/>	Broadcast-Protection ist deaktiviert.
	<input checked="" type="checkbox"/>	Broadcast-Protection ist aktiviert.
Current Speed/Duplex	Aktuelle Übertragungsgeschwindigkeit und aktuelles Übertragungsverfahren	
Speed/Duplex	Übertragungsgeschwindigkeit und Übertragungsverfahren auswählen; Die Auswahlliste wird geräte- und interfaceabhängig generiert. Mit der Auswahl „Autonegotiation“ werden die Verbindungsmodalitäten automatisch mit der Gegenstelle ausgehandelt.	
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.	

### PFC200 G2 - 4-Port, PFC300

Tabelle 139: WBM-Seite „Ethernet Configuration“ – Gruppen „Ethernet Interface Configuration“

Parameter	Bedeutung	
Interface X<n>	Für jedes im Controller vorhandene Interface wird ein eigener Bereich angezeigt.	
Enabled	Interface aktivieren/deaktivieren.	
	<input type="checkbox"/>	Das Interface ist deaktiviert.
	<input checked="" type="checkbox"/>	Das Interface ist aktiviert.
MAC Learning	„MAC Learning“-Funktionalität für das Interface aktivieren/deaktivieren.	
	<input type="checkbox"/>	Die „MAC Learning“-Funktionalität ist deaktiviert.
	<input checked="" type="checkbox"/>	Die „MAC Learning“-Funktionalität ist aktiviert.
Broadcast Protection Enabled	Broadcast-Protection aktivieren/deaktivieren.	
	<input type="checkbox"/>	Broadcast-Protection ist deaktiviert.
	<input checked="" type="checkbox"/>	Broadcast-Protection ist aktiviert.
Multicast Protection Enabled	Multicast-Protection aktivieren/deaktivieren.	
	<input type="checkbox"/>	Multicast-Protection ist deaktiviert.
	<input checked="" type="checkbox"/>	Multicast-Protection ist aktiviert.
Current Speed/Duplex	Aktuelle Übertragungsgeschwindigkeit und aktuelles Übertragungsverfahren	
Speed/Duplex	Übertragungsgeschwindigkeit und Übertragungsverfahren auswählen; Die Auswahlliste wird geräte- und interfaceabhängig generiert. Mit der Auswahl „Autonegotiation“ werden die Verbindungsmodalitäten automatisch mit der Gegenstelle ausgehandelt.	
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.	

#### 7.1.1.3.4 Seite „Configuration of Host and Domain Name“

Auf dieser Seite sind Einstellungen zum Host- und Domain-Namen möglich.

### Gruppe „Hostname“

Tabelle 140: WBM-Seite „Configuration of Host- and Domain Name“ – Gruppe „Hostname“

Parameter	Bedeutung
Currently used	Aktuell verwendeter Hostname
Configured	Optionalen Hostnamen eingeben
[Clear]	Optionalen Hostnamen löschen und Standardwert wiederherstellen
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.

Wenn ein Hostname per DHCP-Antwort geliefert wird, wird dieser im System aktiv. Bei mehreren Netzwerk-Schnittstellen mit DHCP gilt immer der zuletzt empfangene Hostname.

Falls nur der hier konfigurierte Hostname gelten soll, muss die Konfiguration der DHCP-Server so angepasst werden, dass keine Hostnamen in der DHCP-Antwort übertragen werden.

### Gruppe „Domain Name“

Tabelle 141: WBM-Seite „Configuration of Host- and Domain Name“ – Gruppe „Domain Name“

Parameter	Bedeutung
Currently used	Aktuell verwendeter Domainname
Configured	Optionalen Domainnamen eingeben
[Clear]	Optionalen Domainnamen löschen
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.

Wenn ein Domainname per DHCP-Antwort geliefert wird, wird dieser im System aktiv. Bei mehreren Netzwerkschnittstellen mit DHCP gilt immer der zuletzt empfangene Domainname.

Falls nur der hier konfigurierte Domainname gelten soll, muss die Konfiguration der DHCP-Server so angepasst werden, dass keine Domainnamen in der DHCP-Antwort übertragen werden.

#### 7.1.1.3.5 Seite „Routing“

Auf der Seite „Routing“ finden Sie Einstellungen und Informationen zum Routing zwischen den Netzwerkschnittstellen.

### Gruppe „IP Forwarding through multiple interfaces“

Tabelle 142: WBM-Seite „Routing“ – Gruppe „IP Forwarding through multiple interfaces“

Parameter	Bedeutung
Enabled	Weiterleitung von IP-Datenpaketen zwischen unterschiedlichen Netzwerkschnittstellen erlauben
	<input type="checkbox"/> Einstellungen unter „Static Routes“ werden angewendet, ohne dass IP-Datenpakete, die die Steuerung auf einer Netzwerkschnittstelle erreichen, die Steuerung auf einer anderen Netzwerkschnittstelle verlassen dürfen.
	<input checked="" type="checkbox"/> IP-Pakete dürfen zwischen den Interfaces weitergeleitet werden. Ggf. sind weitere Einstellungen erforderlich.
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.

### Gruppe „Custom Routes“

Für jede konfigurierte statische Route wird ein eigener Bereich angezeigt. Wenn keine statischen Routen eingetragen wurden, wird „(no custom routes)“ angezeigt.

Tabelle 143: WBM-Seite „Routing“ – Gruppe „Custom Routes“

Parameter	Bedeutung	
Enabled	Verwendung der ausgewählten Route	
	<input type="checkbox"/>	Die Route wird nicht verwendet.
	<input checked="" type="checkbox"/>	Die Route wird verwendet.
Destination Address	Zieladresse des Teilnehmers	
	default	Es sind beliebige Netzwerkteilnehmer erreichbar.
	Netzwerkadresse	Es ist nur ein bestimmter Teilnehmer oder Teilnehmer aus dem vorgegebenen Adress-Pool erreichbar.
Destination Mask	Subnet-Maske des Teilnehmers Wenn bei Destination-Address „default“ eingetragen ist, muss hier der Wert „0.0.0.0“ eingetragen werden.	
Gateway Address	Adresse des Gateways Ist das Eingabefeld „Interface“ leer, ist hier eine Eingabe erforderlich. Wird im Eingabefeld „Interface“ ein Wert eingetragen, ist die Eingabe hier optional.	
Gateway Metric	Metrik der Route Die Metrik bestimmt bei mehreren Routen gleicher Destination-Address und Destination-Mask, an welches Gateway Netzwerk-Datenpakete zuerst geschickt werden. Routen mit kleinerer Metrik werden bevorzugt. Der kleinste Wert ist 0. Der größte Wert ist $2^{32} - 1 = 4.294.967.295$ .	
Interface	Interface, über das die an die Destination-Address gerichteten Pakete geleitet werden Es können sowohl Bridges (br0 ... br3) als auch Modem (wwan0) oder VPN-Interface-Namen verwendet werden. Ist das Eingabefeld „Gateway Address“ leer, ist hier eine Eingabe erforderlich. Wird im Eingabefeld „Gateway Address“ ein Wert eingetragen, ist die Eingabe hier optional.	
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.	
[Delete]	Ausgewählten Eintrag löschen; Die Schaltfläche ist nur sichtbar, wenn Einträge vorhanden sind.	
[Add]	Neuen Eintrag hinzufügen.	

### Gruppe „Dynamic Routes (assigned by DHCP)“

Hier werden alle über DHCP empfangenen Default-Gateways angezeigt. Default-Gateways, die über DHCP konfiguriert werden, bekommen die Metrik 10, womit sie typischerweise vor den statisch konfigurierten Default-Gateways verwendet werden.

Für jede dynamische Route wird ein eigener Bereich angezeigt. Wenn keine dynamischen Routen über DHCP empfangen wurden, wird „(no dynamic route)“ angezeigt.

### Gruppe „IP Masquerading“

Für jeden Eintrag wird ein eigener Bereich angezeigt.

Tabelle 144: WBM-Seite „Routing“ – Gruppe „IP Masquerading“

Parameter	Bedeutung
Enabled	IP-Masquerading verwenden

Parameter	Bedeutung	
	<input type="checkbox"/>	IP-Masquerading wird nicht verwendet.
	<input checked="" type="checkbox"/>	IP-Masquerading wird verwendet.
Interface	Einen der angegebenen Namen eines Netzwerk-Interface auswählen Über die Auswahl von „other“ ist ein beliebiger Netzwerk-Interface-Name möglich.	
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.	
[Delete]	Ausgewählten Eintrag löschen; Die Schaltfläche ist nur sichtbar, wenn Einträge vorhanden sind.	
[Add]	Neuen Eintrag hinzufügen.	

Ein Eintrag wird nur ins System übertragen, wenn „Enabled“ in der Gruppe „General Routing Configuration“ aktiviert ist. Damit kann eine Voreinstellung getroffen werden, die erst mit der generellen Einschaltung übernommen wird.

### Gruppe „Port Forwarding“

Für jeden Eintrag wird ein eigener Bereich angezeigt.

Tabelle 145: WBM-Seite „Routing“ – Gruppe „Port Forwarding“

Parameter	Bedeutung	
Enabled	Port-Forwarding verwenden	
	<input type="checkbox"/>	Port-Forwarding wird nicht verwendet.
	<input checked="" type="checkbox"/>	Port-Forwarding wird verwendet.
Interface	Einen der angegebenen Namen eines Netzwerk-Interface auswählen Über die Auswahl von „other“ ist ein beliebiger Netzwerk-Interface-Name möglich.	
Port	Port auswählen, auf dem weiterzuleitende Netzwerk-Datenpakete das Produkt erreichen	
Protocol	Protokoll auswählen, welches für das Port-Forwarding berücksichtigt werden soll; Zur Auswahl stehen TCP, UDP oder beide Protokolle.	
Destination Address	Netzwerkadresse des Zielteilnehmers auswählen Diese Adresse ersetzt die ursprüngliche Destination-Adresse des Netzwerk-Datenpakets.	
Destination Port	Port-Nummer des Zielteilnehmers auswählen Dieser Wert ersetzt den ursprünglichen Destination-Port des Netzwerk-Datenpakets.	
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.	
[Delete]	Ausgewählten Eintrag löschen; Die Schaltfläche ist nur sichtbar, wenn Einträge vorhanden sind.	
[Add]	Neuen Eintrag hinzufügen.	

Ein Eintrag wird nur ins System übertragen, wenn „Enabled“ in der Gruppe „General Routing Configuration“ aktiviert ist. Damit kann eine Voreinstellung getroffen werden, die erst mit der generellen Einschaltung übernommen wird.

#### 7.1.1.3.6 Seite „Spanning Tree Protocol“

Auf der Seite „Spanning Tree Protocol“ finden Sie die Einstellungen zu STP/RSTP.

## Gruppe „Status“

In der Gruppe „Status“ werden die aktuellen Werte der aktiven STP/RSTP-Konfiguration angezeigt.

Tabelle 146: WBM-Seite „Spanning Tree Protocol“ – Gruppe „Status“

Parameter	Bedeutung	
Current Status	Aktueller Status	
	<input type="checkbox"/>	STP/RSTP ist nicht aktiv.
	<input checked="" type="checkbox"/>	STP/RSTP ist aktiv.
Current Bridge	Ausgewählte Bridge	
Current Mode	Aktuelles Protokoll	
	STP	Spanning Tree Protocol ist aktiv.
	RSTP	Rapid Spanning Tree Protocol ist aktiv.
Current Priority	Aktuelle Bridge-Priorität	
Current Hello Time (sec)	Aktuelle „Hello“-Zeit in Sekunden	
Current Forward Delay (sec)	Aktuelle „Forward Delay“-Zeit in Sekunden	
Current Max Age (sec)	Aktuelle „Max Age“-Zeit in Sekunden	
Current Max Hops	Aktuelle Max Hops	
Current Path Cost	Aktuelle Path Cost	
Port X[n]	Für jeden Port X[n] der ausgewählten Bridge wird ein eigener Bereich angezeigt. Die Porteinstellungen werden erst angezeigt, nachdem STP/RSTP erfolgreich aktiviert wurde.	
Current Bpdu Filter	Aktueller „Bpdu Filter“-Status	
	<input type="checkbox"/>	Bpdu-Filter ist nicht aktiv.
	<input checked="" type="checkbox"/>	Bpdu-Filter ist aktiv.
Current Bpdu Guard	Aktueller „Bpdu Guard“-Status	
	<input type="checkbox"/>	Bpdu-Guard ist nicht aktiv.
	<input checked="" type="checkbox"/>	Bpdu-Guard ist aktiv.
Current Edge Port	Aktueller Port-Status	
	<input type="checkbox"/>	Port ist kein Edge-Port.
	<input checked="" type="checkbox"/>	Port ist Edge-Port.
Current Root Guard	Aktueller „Root Guard“-Status	
	<input type="checkbox"/>	Root-Guard ist nicht aktiv.
	<input checked="" type="checkbox"/>	Root-Guard ist aktiv.
Current Path Cost	Aktuelle Path-Kosten	
Current Priority	Aktuelle Priorität	
Current Role	Aktuelle Rolle des Ports	
	Designated	Der in jedem LAN-Segment ausgewählte Port, der die niedrigsten Root-Pfadkosten bietet. Je höher die Verbindungsgeschwindigkeit, desto niedriger ist der Kostenwert.
	Disabled	Der Port ist deaktiviert.
Current Status	Aktueller Status des Ports	
	Forwarding	Der Port kann Daten senden und empfangen, MAC-Adressen lernen und Daten an ihr Ziel weiterleiten.

Parameter	Bedeutung	
	Discarding	Der Port gibt keine Daten an andere Switches im Netzwerk weiter und aktualisiert keine MAC-Adresstabellen.

### Gruppe „Parameter Settings“

In der Gruppe „Parameter Settings“ können Sie die Einstellungen für die STP/RSTP-Konfiguration ändern.

Tabelle 147: WBM-Seite „Spanning Tree Protocol“ – Gruppe „Parameter Settings“

Parameter	Bedeutung	
Enabled	Spanning Tree Protocol aktivieren/deaktivieren.	
	<input type="checkbox"/>	Spanning Tree Protocol ist nicht aktiv.
	<input checked="" type="checkbox"/>	Spanning Tree Protocol ist aktiv.
Bridge	Bridge auswählen.	
Mode	Protokoll auswählen;	
	STP	Spanning Tree Protocol
	RSTP	Rapid Spanning Tree Protocol
Priority	Bridge-Priorität einstellen; Zulässige Werte: 1 ... 15	
Hello Time	Hello Time einstellen; Zulässige Werte: 1 ... 19	
Forward Delay	Forward Delay einstellen; Zulässige Werte: 4 ... 30	
Max Age	Max Age einstellen; Zulässige Werte: 6 ... 40	
Max Hops	Max Hops einstellen; Zulässige Werte: 6 ... 40	
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.	
Port X[n]	Für jeden Port X[n] wird ein eigener Bereich angezeigt. Die Porteinstellungen stehen erst zur Verfügung, nachdem STP/RSTP erfolgreich aktiviert wurde.	
Bpdu Filter	Bpdu Filter aktivieren/deaktivieren.	
	<input type="checkbox"/>	Bpdu Filter ist nicht aktiv.
	<input checked="" type="checkbox"/>	Bpdu Filter ist aktiv.
Bpdu Guard	Bpdu Guard aktivieren/deaktivieren.	
	<input type="checkbox"/>	Bpdu Guard ist nicht aktiv.
	<input checked="" type="checkbox"/>	Bpdu Guard ist aktiv.
Edge Port	Port als Edge Port aktivieren/deaktivieren.	
	<input type="checkbox"/>	Port ist kein Edge Port.
	<input checked="" type="checkbox"/>	Port ist Edge Port.
Root Guard	Root Guard aktivieren/deaktivieren.	
	<input type="checkbox"/>	Root Guard ist nicht aktiv.
	<input checked="" type="checkbox"/>	Root Guard ist aktiv.
Path Cost	Path Cost einstellen; Zulässige Werte: 0 ... 65535	

Parameter	Bedeutung
Priority	Priorität einstellen; Zulässige Werte: 0 ...15, Default = 8
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.

### 7.1.1.3.7 Seite „Clock Settings“

Auf dieser Seite sind Einstellungen zu Datum und möglich.

#### Gruppe „Timezone and Format“

Tabelle 148: WBM-Seite „Clock“ – Gruppe „Timezone and Format“

Parameter	Bedeutung	
Timezone	Zeitzone auswählen, Grundeinstellung:	
	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	„East European Time“, BUL, FI, GR, TR, ...
	CST	„China Standard Time“
JST	„Japan/Korea Standard Time“	
TZ String	Oben nicht auswählbare Zeitzone: Name der Zeitzone, Land und Stadt eingeben Gültigen Namen einer Zeitzone ermitteln: <a href="http://www.timeanddate.com/time/map/">http://www.timeanddate.com/time/map/</a>	
Time Format	Zeitformat: 12h / 24h	
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.	

#### Gruppe „UTC Time and Date“

Tabelle 149: WBM-Seite „Clock“ – Gruppe „UTC Time and Date“

Parameter	Bedeutung
UTC Date	Datum
UTC Time	GMT-Uhrzeit
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.

#### Gruppe „Local Time and Date“

Tabelle 150: WBM-Seite „Clock“ – Gruppe „Local Time and Date“

Parameter	Bedeutung
Local Date	Lokales Datum
Local Time	Lokale Uhrzeit
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.

### 7.1.1.3.8 Seite „Configuration of Serial Interface“

Auf dieser Seite sind Einstellungen zur Kommunikationsschnittstelle möglich.

## 7.1.1.3.8.1 PFC100/PFC200

**Gruppe „Current Serial Interface Configuration“**

In dieser Gruppe wird die Applikation angezeigt, der die serielle Schnittstelle aktuell zugewiesen ist sowie der aktuelle Schnittstellenmodus.

Tabelle 151: WBM-Seite „Configuration of Serial Interface“ – Gruppe „Current Serial Interface Configuration“

Parameter	Bedeutung	
Assigned to	Zuordnung der Kommunikationsschnittstelle	
	Unassigned (usage by Applications, Libraries, PLC Runtime)	Die Kommunikationsschnittstelle ist keiner Applikation zugewiesen. Damit kann beispielsweise das CODESYS Programm über Funktionsbausteine darauf zugreifen.
	Linux Console	Die Kommunikationsschnittstelle ist der Linuxkonsole zugewiesen.
Mode	Modus der Kommunikationsschnittstelle	
	RS232	Die Kommunikationsschnittstelle wird im RS-232-Modus betrieben.
	RS485	Die Kommunikationsschnittstelle wird im RS-485-Modus betrieben.

**! ACHTUNG****Sachschaden durch Umschaltung des Owners oder des Modus!**

Durch die Umschaltung können angeschlossene RS-232/RS-485-Geräte beschädigt werden.

- Entfernen Sie die Geräte vor dem Umschalten.

**Gruppe „Assign Owner of Serial Interface“**

Hier können Sie die Applikation auswählen, der die Kommunikationsschnittstelle nach dem nächsten Controller-Reboot zugewiesen wird.

Tabelle 152: WBM-Seite „Configuration of Serial Interface“ – Gruppe „Assign Mode of Serial Interface“

Parameter	Bedeutung
RS232	Die Kommunikationsschnittstelle wird im RS-232-Modus betrieben.
RS485	Die Kommunikationsschnittstelle wird im RS-485-Modus betrieben.
[Submit]	Änderung übernehmen; Die Änderung wird erst nach dem nächsten Neustart wirksam.

**Gruppe „Assign Mode of Serial Interface“**

Hier können Sie die Betriebsart der Kommunikationsschnittstelle auswählen.

Tabelle 153: WBM-Seite „Configuration of Serial Interface“ – Gruppe „Assign Owner of Serial Interface“

Parameter	Bedeutung
Unassigned (usage by Applications, Libraries, PLC Runtime)	Die Kommunikationsschnittstelle wird keiner Applikation zugewiesen.
Linux Console	Die Kommunikationsschnittstelle wird der Linuxkonsole zugewiesen.
[Submit]	Änderung übernehmen; Die Änderung wird erst nach dem nächsten Neustart wirksam.

## 7.1.1.3.8.2 PFC300

**Gruppe „Current Serial Interface Configuration“**

In dieser Gruppe wird der aktuelle Schnittstellenmodus angezeigt.

Tabelle 154: WBM-Seite „Configuration of Serial Interface“ – Gruppe „Current Serial Interface Configuration“

Parameter	Bedeutung	
Mode	Modus der Kommunikationsschnittstelle	
	RS485	Die Kommunikationsschnittstelle wird im RS-485-Modus betrieben.

**Gruppe „Bus Termination“**

Hier können Sie den Busabschluss für die Kommunikationsschnittstelle aktivieren oder deaktivieren.

Tabelle 155: WBM-Seite „Configuration of Serial Interface“ – Gruppe „Bus Termination“

Parameter	Bedeutung	
Termination enabled	Busabschluss aktivieren/deaktivieren.	
	<input type="checkbox"/>	Der Busabschluss ist deaktiviert.
	<input checked="" type="checkbox"/>	Der Busabschluss ist aktiviert.
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.	

**Gruppe „Bias Network“**

Hier können Sie das Bias-Netzwerk für die Kommunikationsschnittstelle einstellen.

Tabelle 156: WBM-Seite „Configuration of Serial Interface“ – Gruppe „Bias Network“

Parameter	Bedeutung
Off	Kein Bias-Netzwerk ist aktiv.
Low	Das Bias-Netzwerk 1 (640 Ohm) ist aktiv.
High	Das Bias-Netzwerk 2 (1210 Ohm) ist aktiv.
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.

**7.1.1.3.9 Seite „Configuration of Service Interface“**

Auf der Seite „Configuration of Service Interface“ finden Sie die Einstellungen zur Service-Schnittstelle.

**Gruppe „Service Interface assigned to“**

Hier wird die Applikation angezeigt, der die Service-Schnittstelle aktuell zugewiesen ist.

**Gruppe „Assign Owner of Service Interface“**

Hier können Sie die Applikation auswählen, der die Service-Schnittstelle nach dem nächsten Controller-Reboot zugewiesen wird.

Tabelle 157: WBM-Seite „Configuration of Service Interface“ – Gruppe „Assign Owner of Service Interface“

Parameter	Bedeutung
WAGO Service Communication	Die Service-Schnittstelle wird für die WAGO Service-Kommunikation bzw. Laufzeitsystem-Kommunikation verwendet.
Linux Console	Die Service-Schnittstelle ist der Linux-Konsole zugewiesen.

Parameter	Bedeutung
Unassigned (usage by Applications, Libraries, PLC Runtime)	Die Service-Schnittstelle ist keiner Applikation zugewiesen. Damit kann beispielsweise das CODESYS Programm über Funktionsbausteine darauf zugreifen.
[Submit]	Änderung übernehmen; Die Änderung wird erst nach dem nächsten Neustart wirksam.

### 7.1.1.3.10 Seite „Create bootable Image“

Auf der Seite „Create bootable Image“ können Sie ein boot-fähiges Image erstellen.

#### Gruppe „Create bootable image from boot device“

Nachdem das mögliche Ziel ermittelt und ausgegeben wurde, wird dieses zunächst überprüft und das Ergebnis unterhalb der Einstellungen angezeigt.

Tabelle 158: WBM-Seite „Create bootable Image“ – Gruppe „Create bootable image from boot device“

Parameter	Bedeutung	
Boot Device	Anzeige des Speichermediums, von dem gebootet wurde	
Destination	Auswahl des Ziels des zu erstellenden Images; Abhängig von welchem Medium gebootet wurde, steht nach dem Boot-Vorgang folgendes Ziel für das zu erstellende Image zur Auswahl:	
	Boot-System:	Zielpartition für „bootable Image“:
	Speicherkarte	Internal Flash
	Interner Speicher	Memory Card
[Start Copy]	Kopiervorgang starten <ul style="list-style-type: none"> <li>Bei positivem Testausgang startet der Vorgang sofort.</li> <li>Wenn Fehler festgestellt wurden, wird eine entsprechende Meldung angezeigt und der Vorgang wird nicht gestartet.</li> <li>Wenn Warnungen vorliegen, werden diese noch einmal angezeigt und Sie müssen bestätigen, dass Sie den Vorgang trotzdem fortsetzen möchten.</li> </ul>	

- Freier Speicher auf dem Ziel-Device:  
Wenn der freie Speicher weniger als 5 % beträgt, wird eine entsprechende Warnung ausgegeben. Sie können den Kopiervorgang trotzdem starten. Wenn der freie Speicher definitiv zu gering ist, wird eine entsprechende Meldung ausgegeben, und der Vorgang kann nicht gestartet werden.
- Device in Benutzung durch CODESYS:  
Wenn das Device durch CODESYS benutzt wird, wird eine entsprechende Warnung ausgegeben. Sie können den Kopiervorgang trotzdem starten, davon wird jedoch abgeraten!

### 7.1.1.3.11 Seite „Firmware Backup“

Auf der Seite „Firmware Backup“ finden Sie die Einstellungen zur Sicherung der Controllerdaten.

#### Gruppe „Firmware Backup“

Tabelle 159: WBM-Seite „Firmware Backup“ – Gruppe „Firmware Backup“

Parameter	Bedeutung
Boot Device	Speichermedium, von dem das Gerät gebootet wurde
Destination	Speicherziel für das Backup
	Memory Card

Parameter	Bedeutung	
	USB-Stick	Die Daten werden auf den USB-Stick geschrieben. Diese Auswahl ist nur bei Produkten mit USB-Anschluss vorhanden. Die Auswahl ist nur aktiv, wenn ein USB-Stick gesteckt ist und nicht von diesem gebootet wurde.
	Network	Die Daten werden im File-System gespeichert und anschließend auf dem PC als Download zur Verfügung gestellt.
PLC Runtime Project	SPS-Laufzeit-Projekt, Bootprojekt und CODESYS Einstellungen sichern.	
	<input type="checkbox"/>	SPS-Laufzeit-Projekt wird nicht gesichert.
	<input checked="" type="checkbox"/>	SPS-Laufzeit-Projekt wird gesichert.
Settings	Geräteeinstellungen sichern.	
	<input type="checkbox"/>	Geräteeinstellungen werden nicht gesichert.
	<input checked="" type="checkbox"/>	Geräteeinstellungen werden gesichert.
System	Betriebssystem des Geräts und Root-Dateisystem sichern.	
	<input type="checkbox"/>	Betriebssystem des Geräts und Root-Dateisystem werden nicht gesichert.
	<input checked="" type="checkbox"/>	Betriebssystem des Geräts und Root-Dateisystem werden gesichert.
Encryption	Daten verschlüsselt sichern.	
	<input type="checkbox"/>	Daten werden unverschlüsselt gesichert.
	<input checked="" type="checkbox"/>	Daten werden verschlüsselt gesichert.
Encryption passphrase	Verschlüsselungspasswort Das Eingabefeld ist nur sichtbar, wenn das Kontrollfeld <b>Encryption</b> markiert ist.	
Confirm passphrase	Verschlüsselungspasswort zur Kontrolle Das Eingabefeld ist nur sichtbar, wenn das Kontrollfeld <b>Encryption</b> markiert ist.	
[Create Backup]	Back-up-Vorgang starten	

### Hinweis

#### Firmwareversion beachten!

Das Wiederherstellen des Betriebssystems (Auswahl „System“) ist nur zulässig und möglich, wenn die Firmwareversionen zum Sicherungs- und Wiederherstellungszeitpunkt gleich sind. Verzichten Sie ggf. auf die Wiederherstellung des Betriebssystems oder gleichen Sie vorher die Firmwareversion an die Firmwareversion zum Sicherungszeitpunkt an.

### Hinweis

#### Nur ein Package zum Netzwerk kopierbar!

Wenn Sie „Network“ als Speicherziel eingestellt haben, ist je Speichervorgang nur ein Package auswählbar.

**i Hinweis****Kein Back-up von Speicherkarte!**

Von der Speicherkarte aus ist ein Back-up auf den internen Flash-Speicher nicht möglich.

**i Hinweis****Back-up-Zeit berücksichtigen**

Das Erzeugen der Back-up-Dateien kann einige Minuten dauern. Stoppen Sie vor dem Back-up-Vorgang das CODESYS Programm, um diese Zeit weiter zu verkürzen.

**7.1.1.3.12 Seite „Firmware Restore“**

Auf der Seite „Firmware Restore“ finden Sie die Einstellungen zur Wiederherstellung der Controllerdaten.

**Gruppe „Firmware Restore“**

Tabelle 160: WBM-Seite „Firmware Restore“ – Gruppe „Firmware Restore“

Parameter	Bedeutung	
Source	Datenquelle für die Wiederherstellung	
	Memory Card	Die Daten werden von der Speicherkarte gelesen. Diese Auswahl ist nur aktiv, wenn eine Speicherkarte gesteckt ist und nicht von dieser gebootet wurde.
	USB-Stick	Die Daten werden vom USB-Stick gelesen. Diese Auswahl ist nur bei Produkten mit USB-Anschluss vorhanden. Die Auswahl ist nur aktiv, wenn ein USB-Stick gesteckt ist und nicht von diesem gebootet wurde.
	Network	Die Daten werden vom PC hochgeladen und wiederhergestellt.
Boot Device	Speichermedium, von dem das Gerät gebootet wurde	
PLC Runtime Project	Name der Back-up-Datei für das CODESYS Projekt; Das Eingabefeld ist nur aktiv, wenn als Datenquelle das Netzwerk ausgewählt ist.	
Settings	Name der Back-up-Datei für die Einstellungen; Das Eingabefeld ist nur aktiv, wenn als Datenquelle das Netzwerk ausgewählt ist.	
System	Name der Back-up-Datei für die Systemdaten und das Root-Dateisystem; Das Eingabefeld ist nur aktiv, wenn als Datenquelle das Netzwerk ausgewählt ist.	
Decryption	Verschlüsselung der Daten	
	<input type="checkbox"/>	Die Daten wurden verschlüsselt gesichert.
	<input checked="" type="checkbox"/>	Die Daten wurden unverschlüsselt gesichert.
Decryption passphrase	Verschlüsselungspasswort; Das Eingabefeld ist nur sichtbar, wenn das Kontrollfeld <b>Decryption</b> markiert ist.	
[Restore]	Wiederherstellvorgang starten	

** Hinweis****Firmwareversion beachten!**

Das Wiederherstellen des Betriebssystems (Auswahl „System“) ist nur zulässig und möglich, wenn die Firmwareversionen zum Sicherungs- und Wiederherstellungszeitpunkt gleich sind. Verzichten Sie ggf. auf die Wiederherstellung des Betriebssystems oder gleichen Sie vorher die Firmwareversion an die Firmwareversion zum Sicherungszeitpunkt an.

** Hinweis****Datengröße darf nicht größer als die interne Laufwerksgröße sein!**

Beachten Sie, dass die Größe der Daten in dem Verzeichnis media/sd/copy die Gesamtgröße des internen Laufwerks nicht überschreiten darf.

** Hinweis****Wiederherstellung nur vom internen Speicher möglich!**

Wenn das Produkt von der Speicherkarte gebootet wurde, ist eine Wiederherstellung der Firmware nicht möglich.

** Hinweis****Reset durch Wiederherstellung**

Durch die Wiederherstellung des Systems, der Einstellungen oder von CODESYS wird ein Reset ausgeführt!

** Hinweis****Verbindungsverlust durch Wiederherstellung!**

Wenn sich durch die Wiederherstellung die Parameter der ETHERNET-Verbindung ändern, kann das WBM anschließend eventuell keine Verbindung mehr zum Produkt aufbauen. Rufen Sie das WBM neu mit der korrekten IP-Adresse des Produktes in der Adresszeile auf.

** Hinweis****Restore-Zeit berücksichtigen**

Der Restore-Vorgang benötigt ca. 2 ... 3 Minuten.  
Nach dem Restore-Vorgang wird der Controller neu gestartet und ist danach wieder einsatzbereit.

**7.1.1.3.13 Seite „Active System“**

Auf dieser Seite sind Einstellungen zur Auswahl der Partition, von der das System gestartet werden soll, möglich.

### Gruppe „Boot Device“

Tabelle 161: WBM-Seite „Active System“ – Gruppe „Boot Device“

Parameter	Bedeutung
Booted from	Speichermedium, von dem gebootet wurde

### Gruppe „System <n> (Internal Flash)“

Tabelle 162: WBM-Seite „Active System“ – Gruppe „System n (Internal Flash)“

Parameter	Bedeutung	
Active	Systemaktivität	
Configured	Systemaktivität nach dem nächsten Reboot-Vorgang	
State	Systemstatus	
	good	Gültiges System
	bad	Ungültiges System, Nutzung nur für Testzwecke
[Activate]	System beim nächsten Reboot-Vorgang starten.	

#### Hinweis

#### Boot-fähiges System bereitstellen!

Auf dem Boot-System muss ein funktionsfähiges Firmware-Backup vorhanden sein!

#### 7.1.1.3.14 Seite „Mass Storage“

Auf der Seite „Mass Storage“ finden Sie Informationen und Einstellungen zu den Speichermedien.

Die Gruppenüberschrift enthält jeweils die Bezeichnung des Speichermediums („Memory Card“ oder „Internal Flash“) und falls dieses Speichermedium die aktive Partition ist, zusätzlich den Text „Active Partition“.

#### Gruppe „Devices“

Für jedes gefundene Speichermedium wird ein Bereich mit Informationen zum Speichermedium angezeigt.

Tabelle 163: WBM-Seite „Mass Storage“ – Gruppe „Devices“

Parameter	Bedeutung
<Device>	Speichermedium
Boot device	Hier wird angezeigt, ob von diesem Speichermedium gebootet wurde.
Volume name	Name des Speichermediums

#### Gruppe „Create new Filesystem on Memory Card“

#### Hinweis

#### Daten werden gelöscht!

Mit dem Formatieren werden die auf dem Speichermedium gespeicherten Daten gelöscht.

Tabelle 164: WBM-Seite „Mass Storage“ – Gruppe „Create new Filesystem on Memory Card“

Parameter	Bedeutung	
IP Source	Format, mit dem das Dateisystem auf der Speicherkarte neu erstellt wird, auswählen	
	Ext4	Das Dateisystem wird im Ext4-Format erstellt. Die Dateien sind unter Windows nicht lesbar!
	FAT	Das Dateisystem wird im FAT-Format erstellt.
Label	Name, den das Speichermedium beim Formatieren erhalten soll, eingeben	
[Start]	Speichermedium formatieren	

#### 7.1.1.3.15 Seite „Software Uploads“

Auf der Seite „Software Uploads“ können Softwarepakete von Ihrem PC auf das Produkt installiert werden.

Tabelle 165: WBM-Seite „Software Uploads“ – Gruppe „Upload new Software“

Parameter	Bedeutung
Software File	Dateiname des ausgewählten Softwarepaketes, solange es noch nicht auf das Produkt übertragen wurde; Wenn Sie noch kein Paket ausgewählt haben, erscheint der Text „Choose ipk file ...“. In diesem Fall klicken Sie das Eingabefeld und wählen Sie eine Datei mit einem Softwarepaket auf Ihrem PC aus.
Force install	
[Install]	Ausgewähltes Paket installieren; Nach dem Installationsvorgang wird die Datei mit dem Softwarepaket wieder vom Produkt gelöscht. Sollte dies durch Fehler bei der Verarbeitung nicht möglich sein, erfolgt das Löschen spätestens beim nächsten Neustart des Produktes.

#### 7.1.1.3.16 Seite „Configuration of Network Services“

Auf dieser Seite sind Einstellungen zu verschiedenen Diensten möglich.

### Hinweis

#### Nicht benötigte Ports und Dienste schließen!

Durch geöffnete Ports können Unbefugte Zugriff auf Ihr Automatisierungssystem erhalten.

- Um die Gefahr von Cyberangriffen zu verringern und damit die Cyber-Security zu erhöhen, schließen Sie alle nicht von Ihrer Applikation benötigten Ports und Dienste in den Steuerungskomponenten (z. B. Port 6626 für WAGO-I/O-CHECK und Port 11740 für CO-DESYS V3).
- Öffnen Sie die Ports und Dienste nur für die Dauer der Inbetriebnahme bzw. Konfiguration.

#### Gruppe „FTP“

Tabelle 166: WBM-Seite „Configuration of Network Services“ – Gruppe „FTP“

Parameter	Bedeutung	
Service active	FTP-Service aktivieren/deaktivieren;	
	<input type="checkbox"/>	Der FTP-Service ist deaktiviert; Werkseinstellung

Parameter	Bedeutung	
	<input checked="" type="checkbox"/>	Der FTP-Service ist aktiviert.
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.	

### Gruppe „FTPES (explicit FTPS)“

Tabelle 167: WBM-Seite „Configuration of Network Services“ – Gruppe „FTPES (explicit FTPS)“

Parameter	Bedeutung	
Service active	FTPES (explicit FTPS)-Service aktivieren/deaktivieren;	
	<input type="checkbox"/>	Der FTPES-Service ist deaktiviert; Werkseinstellung
	<input checked="" type="checkbox"/>	Der FTPES-Service ist aktiviert.
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.	

### Gruppe „HTTP“

Tabelle 168: WBM-Seite „Configuration of Network Services“ – Gruppe „HTTP“

Parameter	Bedeutung	
Service active	HTTP-Service aktivieren/deaktivieren;	
	<input type="checkbox"/>	Der HTTP-Service ist deaktiviert; Werkseinstellung
	<input checked="" type="checkbox"/>	Der HTTP-Service ist aktiviert.
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.	

## Hinweis

### Verbindungsabbruch bei Deaktivierung

Wenn der Service deaktiviert wird, kann die Verbindung zum Produkt unterbrochen werden.

- Rufen Sie die Seite erneut auf.

### Gruppe „HTTPS“

Tabelle 169: WBM-Seite „Configuration of Network Services“ – Gruppe „HTTPS“

Parameter	Bedeutung	
Service active	Status des HTTPS-Service	
	<input type="checkbox"/>	Der HTTPS-Service ist deaktiviert.
	<input checked="" type="checkbox"/>	Der HTTPS-Service ist aktiviert.

### Gruppe „I/O-CHECK“

Tabelle 170: WBM-Seite „Configuration of Network Services“ – Gruppe „I/O-CHECK“

Parameter	Bedeutung	
Service active	WAGO I/O-CHECK-Service aktivieren/deaktivieren;	
	<input type="checkbox"/>	Der WAGO I/O-CHECK-Service ist deaktiviert; Werkseinstellung
	<input checked="" type="checkbox"/>	Der WAGO I/O-CHECK-Service ist aktiviert.

Parameter	Bedeutung
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.

### 7.1.1.3.17 Seite „Configuration of NTP Client“

Auf der Seite „Configuration of NTP Client“ finden Sie die Einstellungen zum NTP-Dienst.

#### Gruppe „NTP Client Configuration“

Tabelle 171: WBM-Seite „Configuration of NTP Client“ – Gruppe „NTP Client Configuration“

Parameter	Bedeutung
Service enabled	Automatische Aktualisierung der Uhrzeit aktivieren/deaktivieren;
	<input type="checkbox"/> Die Aktualisierung der Uhrzeit ist deaktiviert; Werkseinstellung
	<input checked="" type="checkbox"/> Die Aktualisierung der Uhrzeit ist aktiviert.
Update Interval (sec)	Aktualisierungsintervall des Time-Servers eingeben.
Time Server <n>	IP-Adressen der Time-Server eingeben; Es sind maximal 4 Time-Server möglich.
Additionally assigned (DHCP)	Durch DHCP zugewiesene NTP-Server; Wenn kein Time-Server zugewiesen wurde, wird „No additional servers assigned“ angezeigt.
[Update Time]	Uhrzeit aktualisieren
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.

### 7.1.1.3.18 Seite „PLC Runtime Services“

Auf der Seite „PLC Runtime Services“ finden Sie die Einstellungen zu verschiedenen Diensten des Laufzeitsystems.

#### Gruppe „CODESYS V3“

Tabelle 172: WBM-Seite „PLC Runtime Services“ – Gruppe „CODESYS V3“

Parameter	Bedeutung
CODESYS V3 State	Status des Laufzeitsystems
	disabled Das Laufzeitsystem ist deaktiviert.
	enabled Das Laufzeitsystem ist aktiviert.
Webserver Enabled	Webserver für die Webvisualisierung aktivieren/deaktivieren.
	<input type="checkbox"/> Der Webserver ist deaktiviert.
	<input checked="" type="checkbox"/> Der Webserver ist aktiviert.
Separated WebVisu Ports (8080/8081)	CODESYS WebVisu-Ports für HTTP/HTTPS einstellen.
	<input type="checkbox"/> Die CODESYS WebVisu wird auf den Ports 80/443 bereitgestellt (Standard wie WBM).
	<input checked="" type="checkbox"/> Die CODESYS WebVisu wird auf den Ports 8080/8081 bereitgestellt.
Port Authentication Enabled	Log-in für die Verbindung zum Gerät aktivieren/deaktivieren.
	<input type="checkbox"/> Für die Verbindung ist kein Log-in erforderlich.

Parameter	Bedeutung	
	<input checked="" type="checkbox"/>	Für die Verbindung ist ein Log-in erforderlich. Der Standard-Benutzername ist admin und das Passwort ist das unter „General Configuration“ angegebene Passwort.
Webserver Port Authentication Enabled	<input type="checkbox"/>	Für den Aufruf der Webvisualisierung ist kein Log-in erforderlich.
	<input checked="" type="checkbox"/>	Für den Aufruf der Webvisualisierung ist ein Log-in erforderlich. Der Standard-Benutzername ist admin und das Passwort ist das unter „General Configuration“ angegebene Passwort.
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.	

### 7.1.1.3.19 Seite „SSH Server Settings“

Auf der Seite „SSH Server Settings“ finden Sie die Einstellungen zum SSH-Dienst.

#### Gruppe „SSH Server“

Tabelle 173: WBM-Seite „SSH Server Settings“ – Gruppe „SSH Server“

Parameter	Bedeutung	
Service active	<input type="checkbox"/>	SSH-Server-Dienst aktivieren/deaktivieren. Der SSH-Server-Dienst ist deaktiviert.
	<input checked="" type="checkbox"/>	Der SSH-Server-Dienst ist aktiviert.
Port Number	Port-Nummer eingeben.	
Allow root login	Root-Zugriff sperren oder erlauben.	
Allow password login	Passwortabfrage aktivieren oder deaktivieren.	
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.	

### 7.1.1.3.20 Seite „DHCP Server Configuration“

Auf der Seite „DHCP Server Configuration“ finden Sie die Einstellungen zum DHCP-Dienst.

Für jede konfigurierte Bridge wird eine eigene Gruppe angezeigt.

#### Gruppe „DHCP Server Configuration Bridge <n>“

Tabelle 174: WBM-Seite „DHCP Server Configuration“ – Gruppe „DHCP Server Configuration Bridge <n>“

Parameter	Bedeutung	
Service active	<input type="checkbox"/>	DHCP-Server-Dienst für die Bridge <n> aktivieren/deaktivieren; Der DHCP-Server-Dienst für die Bridge <n> ist nicht aktiviert.
	<input checked="" type="checkbox"/>	Der DHCP-Server-Dienst für die Bridge <n> ist aktiviert.
Start IP for Range	Anfangswert des verfügbaren IP-Adressbereichs eingeben.	
End IP for Range	Endwert des verfügbaren IP-Adressbereichs eingeben.	
Lease time (min)	Ausleihzeit in Minuten eingeben. Werkseinstellung: 120 Minuten	

Parameter	Bedeutung
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.
Static Hosts	Statische Zuordnungen von MAC-IDs oder Hostnamen zu IP-Adressen; Wenn keine Zuordnung vorhanden ist, wird „No static hosts configured“ angezeigt.
[Delete]	Ausgewählten Eintrag löschen; Die Schaltfläche ist nur sichtbar, wenn Einträge vorhanden sind.
Add Static Host	Statische Zuordnungen von MAC-Adressen oder Hostnamen zu IP-Adressen hinzufügen; Es sind max. 15 Zuordnungen möglich.
MAC Address or Hostname	MAC-Adresse oder Hostnamen eingeben; Z. B. „01:02:03:04:05:06=192.168.1.20“ oder „hostname=192.168.1.20“.
IP Address	IP-Adresse eingeben.
[Add]	Neuen Eintrag hinzufügen.

### 7.1.1.3.21 Seite „Configuration of DNS Server“

Auf dieser Seite sind Einstellungen zum DNS-Dienst möglich.

#### Gruppe „DNS Server“

Tabelle 175: WBM-Seite „Configuration of DNS Server“ – Gruppe „DNS Server“

Parameter	Bedeutung	
Service active	DNS-Server-Dienst aktivieren/deaktivieren;	
	<input type="checkbox"/>	Der DNS-Server-Dienst ist deaktiviert.
	<input checked="" type="checkbox"/>	Der DNS-Server-Dienst ist aktiviert.
Mode	Betriebsart einstellen;	
	Proxy	Anfragen werden zur Durchsatzoptimierung zwischengespeichert.
	Relay	Alle Anfragen werden direkt weitergeleitet.
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.	
Static Hosts	Statische Zuordnungen von Hostnamen zu IP-Adressen; Wenn keine Zuordnung vorhanden ist, wird „No static hosts configured“ angezeigt.	
[Delete]	Ausgewählten Eintrag löschen; Die Schaltfläche ist nur sichtbar, wenn Einträge vorhanden sind.	
Add Static Host	Statische Zuordnungen von IP-Adressen zu Hostnamen hinzufügen; Es sind max. 10 Zuordnungen möglich.	
IP Address	IP-Adresse eingeben; Z. B. „192.168.1.20:hostname“	
Hostname	Hostnamen eingeben.	
[Add]	Neuen Eintrag hinzufügen.	

### 7.1.1.3.22 Seite „Status overview“

Auf der Seite „Status overview“ finden Sie Informationen zum Cloud-Zugang.

#### Gruppe „Connection <n>“

Für jeden Cloud-Zugang wird eine eigene Gruppe angezeigt.

Tabelle 176: WBM-Seite „Overview“ – Gruppe „Connection &lt;n&gt;“

Parameter	Bedeutung
Operation	Status der Cloud-Connectivity-Applikation
Data from PLC Runtime	Anzahl der Data-Collections, die seitens der IEC-Applikation für die Übertragung zur Cloud registriert wurden
Cloud Connection	Status der Verbindung zum Cloud-Dienst
Heartbeat	Aktuell konfiguriertes Heartbeat-Intervall in Sekunden
Telemetry data transmission	Status der Datenübertragung
Cache fill level (QoS 1 and 2)	Füllstand des Speichers für ausgehende Nachrichten in Prozent

### 7.1.1.3.23 Seite „Configuration of Connection <n>“

Auf dieser Seite sind Einstellungen und Informationen zum Cloud-Zugang möglich.

Für jeden Cloud-Zugang wird eine eigene Seite angezeigt.

#### Gruppe „Configuration“

Die angezeigten Parameter sind abhängig von der eingestellten Cloud-Plattform und ggf. von weiteren Einstellungen in dieser Gruppe.

Die Abhängigkeiten werden in einer separaten Tabelle dargestellt.

Tabelle 177: WBM-Seite „Configuration of Connection &lt;n&gt;“ – Gruppe „Configuration“

Parameter	Bedeutung
Enabled	Cloud-Connectivity-Funktionalität aktivieren/deaktivieren
Cloud platform	Cloud-Plattform
Hostname	Hostname oder IP-Adresse für die ausgewählte Cloud-Plattform
ID Scope	Endpunkt für den Azure Gerätebereitstellungsdienst (DPS)
Registration ID	Registrierungs-ID für den Azure Gerätebereitstellungsdienst (DPS)
Port number	Port-Nummer, zu dem eine Verbindung aufgebaut werden soll  Typische Werte: <ul style="list-style-type: none"> <li>▪ 8883 für verschlüsselte Verbindungen</li> <li>▪ 1883 für unverschlüsselte Verbindungen</li> </ul>
Device ID	Device-ID für die ausgewählte Cloud-Plattform
Client ID	Client-ID für die ausgewählte Cloud-Plattform
Authentication	Authentifizierungsmethode, z. B. „Shared Key Acces“, „X.509 Certificate“
Activation Key	Aktivierungsschlüssel für die ausgewählte Cloud-Plattform
Clean Session	Clean-Session bei der Verbindung zum Cloud-Dienst aktivieren  Clean-Session aktiv: Informationen und Nachrichten zu dieser Verbindung beim Cloud-Dienst nicht persistent gespeichert
TLS	Verwendung einer TLS-Verschlüsselung für die Verbindung zur Cloud-Plattform aktivieren/deaktivieren  Amazon Web Services (AWS) verwendet TLS
CA file	Pfad zu der im PEM-Format enkodierten Datei, die das für den Aufbau einer verschlüsselten Verbindung zu verwendende und vertrauenswürdige CA-Zertifikat enthält  Standardwert: CA-Zertifikat /etc/ssl/certs/ca-certificates.crt
User	Benutzername
Password	Passwort
Certification file	Pfad zu der im PEM-Format enkodierten Datei, die zur Authentisierung gegenüber dem Cloud-Dienst genutzt wird

Parameter	Bedeutung
Key file	Pfad zu der im PEM-Format enkodierten Datei, welche den privaten Schlüssel für die Authentisierung gegenüber dem Cloud-Dienst enthält
Use websockets	Verbindungsaufbau zur Cloud-Plattform mittels WebSocket-Protokoll über den Port 443 aktivieren/deaktivieren  Wenn deaktiviert: Verbindungsaufbau zur Cloud-Plattform mittels MQTT-Protokoll über den Port 8883
HTTP Proxy Host	Hostname oder IP-Adresse des Proxys
HTTP Proxy Port	Portnummer des Proxys
HTTP Proxy User	Name des Proxy-Benutzers
HTTP Proxy Password	Passwort des Proxy-Benutzers
Use compression	Datenkomprimierung mittels GZIP-Komprimierung aktivieren/deaktivieren
Data Protocol	Daten-Protokoll
Cache mode	Speicherort des Caches für die Datentelegramme  Auswahlfeld nur aktiv, wenn eine korrekt formatierte SD-Karte gesteckt ist  Weitere Informationen: Anwendungshinweis A500920
Last Will	Last-Will-Nachricht aktivieren/deaktivieren  Nach Aktivierung erscheinen nachfolgend zusätzliche Eingabefelder
(Last Will) Topic	Topic, unter welchem die Last-Will-Nachricht versendet werden soll
(Last Will) Message	Nachricht, die als Last-Will-Nachricht versendet werden soll
(Last Will) QoS	„Quality of Service“ (QoS) der Last-Will-Nachricht
(Last Will) Retain	Letzte unter einem Topic gesendete Last-Will-Nachricht vom Broker als gespeicherte Nachricht (Retained Message) aktivieren/deaktivieren
Device info	Device-Info-Nachricht, welche den Cloud-Dienst über die grundlegende Konfiguration des Controllers informiert, aktivieren/deaktivieren  Weitere Informationen: Anwendungshinweis A500920
Device status	Device-State-Nachrichten, welche den Cloud-Dienst über Änderungen des Betriebsartenschalters sowie der LEDs informiert, aktivieren/deaktivieren  Weitere Informationen: Anwendungshinweis A500920
Standard commands	Integrierte Standardkommandos aktivieren/deaktivieren  Weitere Informationen: Anwendungshinweis A500920  Wenn deaktiviert: Nur die im IEC-Programm definierten Kommandos unterstützt
Application property template	Eigenes Property für die einzelnen MQTT-Nachrichten zur Azure-Cloud erstellen  Parameter optional, d. h., wenn das Feld leer gelassen wird, wird dieses Property nicht mitgesendet  Platzhalter zur Erstellung: <ul style="list-style-type: none"> <li>• &lt;m&gt;: Nachrichtentype</li> <li>• &lt;p&gt;: Protokoll-Version</li> <li>• &lt;d&gt;: DeviceId</li> </ul> Beispiele: <ul style="list-style-type: none"> <li>• MyKey=HelloWorld_&lt;m&gt;</li> <li>• TestKey=&lt;m&gt;/&lt;p&gt;/&lt;d&gt;</li> <li>• DeviceId=&lt;d&gt;</li> </ul>
[Submit]	Änderung übernehmen; Die Änderung wird erst nach dem nächsten Neustart wirksam.

Die nachfolgenden Tabellen zeigen die Abhängigkeiten der Auswahl- und Eingabefelder sowie der möglichen Einstellungen.

Tabelle 178: Anzeige der Auswahl- und Eingabefelder abhängig von der ausgewählten Cloud-Plattform

Auswahl- oder Eingabefeld	Cloud-Plattform					
	WAGO Cloud	Azure	MQTT Any-Cloud	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	
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
X: Sichtbar und aktiv						
(X): Sichtbar, aber nicht aktiv						
X1: Sichtbar und aktiv, abhängig vom ausgewählten Datenprotokoll						
X2: Sichtbar und aktiv, abhängig von der ausgewählten Authentifizierung						
X3: Sichtbar und aktiv, wenn „Last Will“ eingeschaltet ist						
(X3): Sichtbar, aber nicht aktiv, wenn „Last Will“ eingeschaltet ist						
X4: Aktiv, wenn „Use websockets“ eingeschaltet ist						
X5: Sichtbar und aktiv, wenn „Use websockets“ eingeschaltet ist und wenn als „Proxy Type“ „HTTP“ eingestellt ist						

Tabelle 179: Auswahlmöglichkeit des Datenprotokolls abhängig von der ausgewählten Cloud-Plattform

Datenprotokoll	Cloud-Plattform					
	WAGO Cloud	Azure	MQTT Any-Cloud	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: Auswahl möglich						
(X): Fest eingestellt						

Tabelle 180: Anzeige der Auswahl- und Eingabefelder abhängig vom ausgewählten Datenprotokoll

Auswahl- oder Eingabefeld	Datenprotokoll			
	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: Sichtbar und aktiv				

Tabelle 181: Auswahlmöglichkeit des Cache-Modes abhängig vom ausgewählten Datenprotokoll

Cache-Mode	Datenprotokoll			
	WAGO Protocol	WAGO Protocol 1.5	Native MQTT	Sparkplug payload B
RAM	X	X	X	(X)
SD-Card	X1	X1	X1	
X: Auswahl möglich				
X1: Auswahl nur möglich, wenn "Compression" nicht eingeschaltet ist				
(X): Fest eingestellt				

Tabelle 182: Anzeige der Eingabefelder abhängig von der ausgewählten Authentifizierung

Auswahl- oder Eingabefeld	Authentifizierung	
	Shared Access Key	X.509 Certificate
Activation Key	X	
Certification file		X
Key file		X
X: Sichtbar und aktiv		

#### 7.1.1.3.24 Seite „Controls Settings“

Auf der Seite „Controls Settings“ im Register „Configuration“ finden Sie Einstellungen und Informationen zur Aktivierung/Deaktivierung des Betriebsartenschalters und des Reset-Tasters.

Tabelle 183: WBM-Seite „Controls Settings“ – Gruppe „OMS Controls“

Parameter	Bedeutung	
Current Mode	Aktueller Status der Funktionalität des Betriebsartenschalters und des Reset-Tasters	
	Inactive	Der Controller ignoriert jede Betätigung des Betriebsartenschalters und des Reset-Tasters.
	Active	Controller reagiert auf eine Betätigung des Betriebsartenschalters und des Reset-Tasters.
Activate	Aktivierung/Deaktivierung des Betriebsartenschalters und des Reset-Tasters	
	<input type="checkbox"/>	Betriebsartenschalter und Reset-Taster deaktivieren.
	<input checked="" type="checkbox"/>	Betriebsartenschalter und Reset-Taster aktivieren.
[Submit]	Änderung übernehmen; Die Änderung wird erst nach dem nächsten Neustart wirksam.	

### Hinweis

**Bei deaktiviertem Betriebsartenschalter wird ein geladenes CODESYS Boot-Projekt automatisch nach dem Neustart des Produktes ausgeführt!**

Das Stoppen und Zurücksetzen einer laufenden Applikation ist bei deaktiviertem Betriebsartenschalter nur über die CODESYS Entwicklungsumgebung möglich.

#### 7.1.1.3.25 Seite „Configuration of general SNMP parameters“

Auf dieser Seite sind Einstellungen zu allgemeine Einstellungen zu SNMP möglich.

##### Gruppe „General SNMP Configuration“

Tabelle 184: WBM-Seite „Configuration of general SNMP parameters“ – Gruppe „General SNMP Configuration“

Parameter	Bedeutung	
Service active	SNMP-Dienst aktivieren/deaktivieren;	
	<input type="checkbox"/>	Der SNMP-Dienst ist deaktiviert.
	<input checked="" type="checkbox"/>	Der SNMP-Dienst ist aktiviert.
Name of Device	Produktname (sysName) eingeben.	
Description	Produktbeschreibung (sysDescription) eingeben.	
Physical Location	Standort des Produktes (sysLocation) eingeben.	
Contact	E-Mail-Kontaktadresse (sysContact) eingeben.	
ObjectID	Object-ID eingeben.	
[Submit]	Änderung übernehmen; Die Änderung wird erst nach dem nächsten Neustart wirksam.	

#### 7.1.1.3.26 Seite „Configuration of SNMP v1/v2c Parameters“

Auf der Seite „Configuration of SNMP v1/v2c Parameters“ finden Sie die Einstellungen zu SNMP v1/v2c.

### Gruppe „Communities“

Tabelle 185: WBM-Seite „Configuration of SNMP v1/v2c Parameters“ – Gruppe „Communities“

Parameter	Bedeutung
Name	Community-Name für die SNMP-Manager-Konfiguration
Access	Zugriffsrechte für die Community; Mögliche Werte sind: <ul style="list-style-type: none"> <li>• ReadOnly</li> <li>• ReadWrite</li> </ul>
[Delete]	Ausgewählten Eintrag löschen; Die Schaltfläche ist nur sichtbar, wenn Einträge vorhanden sind.
[Add]	Neuen Eintrag hinzufügen.

### Gruppe „Trap Receivers“

Tabelle 186: WBM-Seite „Configuration of SNMP v1/v2cparameters“ – Gruppe „Trap Receivers“

Parameter	Bedeutung
Host	Hostname oder IP-Adresse des Trap-Empfängers (Managementstation)
Community Name	Community-Name für die Trap-Empfänger-Konfiguration
Version	SNMP-Version, über welche die Traps gesendet werden sollen; Mögliche Werte sind: <ul style="list-style-type: none"> <li>• v1</li> <li>• v2c</li> </ul>
[Delete]	Ausgewählten Eintrag löschen; Die Schaltfläche ist nur sichtbar, wenn Einträge vorhanden sind.
[Add]	Neuen Eintrag hinzufügen.

#### 7.1.1.3.27 Seite „Configuration of SNMP v3 Parameters“

Auf der Seite „Configuration of SNMP v3 Parameters“ finden Sie die Einstellungen zu SNMP v3.

### Gruppe „Users“

Tabelle 187: WBM-Seite „Configuration of SNMP v3 Parameters“ – Gruppe „Users“

Parameter	Bedeutung
Security Authentication Name	Benutzername
Authentication Type	Authentifizierungstyp für die SNMP-v3-Pakete; Mögliche Werte sind: <ul style="list-style-type: none"> <li>• Keine Authentifizierung („None“)</li> <li>• Message Digest 5 („MD5“)</li> <li>• Secure Hash Algorithm („SHA“, „SHA224“, „SHA256“, „SHA384“, „SHA512“)</li> </ul>
Authentication Key	Passwort für die Authentifizierung
Privacy	Verschlüsselungsalgorithmus für die SNMP-Nachricht; Mögliche Werte sind: <ul style="list-style-type: none"> <li>• Keine Verschlüsselung („None“)</li> <li>• Data Encryption Standard („DES“)</li> <li>• Advanced Encryption Standard („AES“, „AES128“, „AES192“, „AES192C“, „AES256“, „AES256C“)</li> </ul>
Privacy Key	Verschlüsselungscode
Access	Zugriffsrechte für den v3-User; Mögliche Werte sind <ul style="list-style-type: none"> <li>• ReadOnly</li> <li>• ReadWrite</li> </ul>
[Delete]	Ausgewählten Eintrag löschen; Die Schaltfläche ist nur sichtbar, wenn Einträge vorhanden sind.

Parameter	Bedeutung
[Add]	Neuen Eintrag hinzufügen.

### Gruppe „Trap Receivers“

Tabelle 188: WBM-Seite „Configuration of SNMP v3 Parameters“ – Gruppe „Trap Receivers“

Parameter	Bedeutung
Security Authentication Name	Benutzername
Authentication Type	Authentifizierungstyp für die SNMP-v3-Pakete; Mögliche Werte sind: <ul style="list-style-type: none"> <li>Keine Authentifizierung („None“)</li> <li>Message Digest 5 („MD5“)</li> <li>Secure Hash Algorithm („SHA“, „SHA224“, „SHA256“, „SHA384“, „SHA512“)</li> </ul>
Authentication Key	Passwort für die Authentifizierung
Privacy	Verschlüsselungsalgorithmus für die SNMP-Nachricht; Mögliche Werte sind: <ul style="list-style-type: none"> <li>Keine Verschlüsselung („None“)</li> <li>Data Encryption Standard („DES“)</li> <li>Advanced Encryption Standard („AES“, „AES128“, „AES192“, „AES192C“, „AES256“, „AES256C“)</li> </ul>
Privacy Key	Verschlüsselungscode
Host	Hostname oder IP-Adresse des v3-Trap-Empfängers
[Delete]	Ausgewählten Eintrag löschen; Die Schaltfläche ist nur sichtbar, wenn Einträge vorhanden sind.
[Add]	Neuen Eintrag hinzufügen.

#### 7.1.1.3.28 Seite „Commissioning Settings“

Auf der Seite „Commissioning Settings“ finden Sie Informationen und Einstellungen zum „Commissioning Agent“-Dienst.

### Gruppe „Commissioning“

Tabelle 189: WBM-Seite „Commissioning Settings“ – Gruppe „Commissioning“

Parameter	Bedeutung
Service Enabled	„Commissioning Agent“-Dienst aktivieren/deaktivieren;
	<input type="checkbox"/> Der „Commissioning Agent“-Dienst ist deaktiviert.
	<input checked="" type="checkbox"/> Der „Commissioning Agent“-Dienst ist aktiviert.
Commissioning State	Aktueller Status des „Commissioning Agent“-Dienstes
	inactive Der Dienst ist nicht aktiv.
	searching Der Dienst sucht nach einem Server.
	requesting Der Dienst hat einen Server gefunden und versucht sich zu verbinden.
	awaiting response Der Dienst wartet darauf, vom Server angenommen zu werden.
	no server found Der Dienst hat innerhalb der gegebenen Zeit von fünf Minuten keinen validen Server gefunden. Um die Suche erneut zu starten, muss das Gerät neu gestartet werden.
	processing Der Dienst startet die Installation der vom Server erhaltenen Pakete.
	error exit Der Dienst hat die Installation aufgrund eines internen Fehlers abgebrochen.

Parameter	Bedeutung	
	success	Der Dienst hat die Installation erfolgreich abgeschlossen.
Connected Server	Domain des Servers, mit dem das Produkt verbunden ist; Ist das Produkt nicht verbunden, wird „-“ angezeigt.	
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.	

### 7.1.1.3.29 Seite „Docker Settings“

Auf der Seite „Docker Settings“ finden Sie die Einstellungen zum Dienst „Docker“.

#### Gruppe „Docker Status“

Tabelle 190: WBM-Seite „Docker Settings“ – Gruppe „Docker Status“

Parameter	Bedeutung	
Current State	Aktueller Status des Dienstes „Docker“	
	stopped	Der Dienst „Docker“ ist gestoppt.
	running	Der Dienst „Docker“ ist aktiv.
Service Enabled	Dienst „Docker“ aktivieren/deaktivieren;	
	<input type="checkbox"/>	Der Dienst „Docker“ ist deaktiviert.
	<input checked="" type="checkbox"/>	Der Dienst „Docker“ ist aktiviert.
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.	

### 7.1.1.3.30 Seite „WBM User Configuration“

Auf der Seite „WBM User Configuration“ finden Sie die Einstellungen zur User-Administration.

#### Gruppe „Change Passwords“

##### Hinweis

#### Passwörter ändern!

Die im Auslieferungszustand eingestellten Standardpasswörter sind in dieser Betriebsanleitung dokumentiert und bieten so keinen hinreichenden Schutz.

- Ändern Sie die Passwörter entsprechend Ihren Erfordernissen.

##### Hinweis

#### Zulässige Zeichen für Passwörter

Passwörter dürfen nur die folgenden Zeichen enthalten:

Kleinbuchstaben (a ... z), Großbuchstaben (A ... Z), Ziffern (0 ... 9) und Sonderzeichen (! " # \$ % & ' ( ) \* + , . / : ; < = > ? @ [ ] ^ \_ ` { } | ~ -).

**i Hinweis****Zulässige Zeichen für WBM-Passwörter beachten!**

Werden außerhalb des WBM (z. B. über CBM) Passwörter mit unzulässigen Zeichen für das WBM eingestellt, ist ein Zugriff auf die WBM-Seiten nicht mehr möglich!

Tabelle 191: WBM-Seite „WBM User Configuration“ – Gruppe „Change Passwords“

Parameter	Bedeutung
Old Password	Aktuell verwendetes Passwort zur Authentifizierung eingeben.
New Password	Neues Passwort eingeben.
Confirm Password	Neues Passwort zur Kontrolle erneut eingeben.
[Set Password]	Neues Passwort übernehmen

**i Hinweis****Übergreifende Rechte der WBM-Benutzer**

Die WBM-Benutzer „admin“ und „user“ besitzen über das WBM hinausgehende Rechte, um das System zu konfigurieren und Software zu installieren.

**7.1.1.4 Registerkarte „Fieldbus“****7.1.1.4.1 Seite „OPC UA Configuration“**

Auf der Seite „OPC UA Configuration“ finden Sie die Einstellungen zum OPC-UA-Dienst.

**Gruppe „OPC UA Server Configuration“**

Tabelle 192: WBM-Seite „OPC UA Configuration“ – Gruppe „OPC UA Server Configuration“

Parameter	Bedeutung	
Enabled	OPC UA-Server aktivieren oder deaktivieren.	
	<input type="checkbox"/> Der OPC UA-Server ist deaktiviert.	
	<input checked="" type="checkbox"/> Der OPC UA-Server ist aktiviert.	
Log Level	Log-Levels auswählen; Die Auswahl des Log Levels beeinflusst die Reaktionszeit des Servers. Wählen Sie daher nur den minimal benötigten Level aus, z. B. „Debug“ nur für tiefgreifende Analysen. Folgende Werte sind einstellbar:	
	Error	Es werden nur Fehlermeldungen ausgegeben.
	Warning	Es werden Fehlermeldungen und Warnmeldungen ausgegeben.
	Info	Es werden Fehlermeldungen, Warnmeldungen und Statusmeldungen ausgegeben.
	Debug	Es werden Fehlermeldungen, Warnmeldungen, Statusmeldungen und zusätzlich Debug-Meldungen ausgegeben.
Ctrl Configuration Name	Konfigurationsnamen, den der Controller innerhalb des PLC Open Device Sets erhält, eingeben.	
[Submit]	Änderung übernehmen; Die Änderung wird erst nach dem nächsten Neustart wirksam.	

### Gruppe „OPC UA Server Security Settings“

Tabelle 193: WBM-Seite „OPC UA Configuration“ – Gruppe „OPC UA Server Security Settings“

Parameter	Bedeutung	
Anonymous Access	Anonymen Zugriff auf den Server sperren/zulassen.	
	<input type="checkbox"/>	Ein anonymer Zugriff ist nicht zulässig.
	<input checked="" type="checkbox"/>	Ein anonymer Zugriff ist zulässig; Dies setzt voraus, dass die Portauthentifizierung der Runtime ebenfalls deaktiviert ist/wird.
Allow Password On Plaintext	Übertragung des Passworts im lesbaren Format	
	<input type="checkbox"/>	
	<input checked="" type="checkbox"/>	
Security Modes	Security Mode des OPC UA Servers; Je nach Auswahl der Betriebsart stehen verschiedene OPC UA Endpoints zum Verbindungsaufbau zur Verfügung.	
	None	Lediglich der OPC UA Endpoint <b>None</b> wird aktiviert. Dieser ermöglicht eine ungesicherte Verbindung zum OPC UA Server.
	None + Sign + SignAndEncrypt	Die Endpoints <b>None</b> , <b>Sign</b> und <b>SignAndEncrypt</b> stehen zur Verfügung. <b>Sign</b> stellt einen Endpoint zur Verfügung, der über ein Passwort geschützt ist. <b>SignAndEncrypt</b> stellt einen Endpoint zur Verfügung, der neben einem Passwort auch eine Verschlüsselung ermöglicht.
	Sign + SignAndEncrypt	Die Endpoints <b>Sign</b> und <b>SignAndEncrypt</b> stehen zur Verfügung.
	SignAndEncrypt	Nur der Endpoint <b>SignAndEncrypt</b> steht zur Verfügung.
Security Policies	Auswahl der Security Policies; Hierüber wird die Verschlüsselungsstärke des OPC UA Servers eingestellt. Zur Auswahl stehen dabei: Aes128Sha256RsaOaep and better, Basic256Sha256 and better, Aes256Sha256RsaPss.	
[Submit]	Änderung übernehmen; Die Änderung wird erst nach dem nächsten Neustart wirksam.	

#### 7.1.1.4.2 Seite „BACnet Status“

Auf der Seite „BACnet Status“ werden für den Feldbus BACnet und die BACnet Lizenz spezifische Informationen über Ihr Produkt angezeigt.

### Gruppe „BACnet Information“

Tabelle 194: WBM-Seite „BACnet Status“ – Gruppe „BACnet Information“

Parameter	Bedeutung	
State	BACnet Feldbusstatus	
	<input type="checkbox"/>	Feldbus BACnet ist deaktiviert
	<input checked="" type="checkbox"/>	Feldbus BACnet ist aktiviert
Mode	BACnet Betriebsmodus	
	ip	Kommunikation über BACnet/IP
	sc	Kommunikation über BACnet/SC
Version	Installierte BACnet Version	
Status Info	BACnet Feldbusstatus	

Parameter	Bedeutung
Device-ID	Aktuelle Device-ID des Produkts

### Gruppe „BACnet License“

Tabelle 195: WBM-Seite „BACnet Status“ – Gruppe „BACnet License“

Parameter	Bedeutung
Type	Anzeige der BACnet Lizenzen
User Objects	Anzeige der Anzahl der vorhandenen sowie der mit der Lizenz möglichen BACnet Objekte

### Gruppe „BACnet Data Link“

Tabelle 196: WBM-Seite „BACnet Status“ – Gruppe „BACnet Data Link“

Parameter	Bedeutung
Connection Info	Anzeige des Verbindungsstatus

#### 7.1.1.4.3 Seite „BACnet Configuration“

Auf dieser Seite können Sie für den Feldbus BACnet-spezifische Einstellungen vornehmen.

### Gruppe „Restart“

Tabelle 197: WBM-Seite „BACnet Data Link“ – Gruppe „BACnet Restart“

Parameter	Bedeutung
[Restart]	Neustart des BACnet Dienstes

### Gruppe „BACnet Service“

Tabelle 198: WBM-Seite „BACnet Configuration“ – Gruppe „BACnet Service“

Parameter	Bedeutung
Service active	Feldbus BACnet aktivieren/deaktivieren.
	<input type="checkbox"/> BACnet ist deaktiviert.
	<input checked="" type="checkbox"/> BACnet ist aktiviert.
Mode	Hier wählen Sie den BACnet Betriebsmodus aus.
	ip Kommunikation über BACnet/IP
	sc Kommunikation über BACnet/SC
Who-Is online interval time (sec)	Zeitlicher Abstand der Controller-Anfragen auf den Feldbus, welche weiteren Teilnehmer online sind (minimal: 60 sec).
Broadcast I-Am answer	Aktivieren/deaktivieren, dass die I-Am-Nachrichten des Gerätes an die BACnet Broadcast-Adresse gesendet werden.
	<input type="checkbox"/> I-Am-Nachrichten werden nicht an die BACnet Broadcast-Adresse gesendet.
	<input checked="" type="checkbox"/> I-Am-Nachrichten werden an die BACnet Broadcast-Adresse gesendet.
[Submit]	Änderung übernehmen; Die Änderung wird erst nach dem nächsten Neustart des Controllers oder einem BACnet Restart wirksam.

### Gruppe „BACnet Data“

Tabelle 199: WBM-Seite „BACnet Configuration“ – Gruppe „BACnet Data“

Parameter	Bedeutung
Delete Persistence Data	Persistente BACnet-Daten werden beim nächsten Neustart gelöscht.
Reset all BACnet Data and Settings to Default	BACnet-spezifische Einstellungen und Daten werden beim nächsten Neustart auf Werkseinstellungen zurückgesetzt.
[Submit]	Änderung übernehmen; Die Änderung wird erst nach dem nächsten Neustart des Controllers oder einem BACnet Restart wirksam.
override.xml Chose file ...	Auswahl der gewünschten Datei auf dem PC
[Upload]	Übertragen der ausgewählten Datei vom PC zum Controller

### Gruppe „BACnet Log Level“

Tabelle 200: WBM-Seite „BACnet Configuration“ – Gruppe „BACnet Log Level“

Parameter	Bedeutung
Error	<input type="checkbox"/> Error-Logausgaben aktivieren/deaktivieren. Error-Logeinträge werden nicht ausgegeben.
	<input checked="" type="checkbox"/> Error-Logausgaben aktivieren/deaktivieren. Error-Logeinträge werden ausgegeben.
Warning	<input type="checkbox"/> Warning-Logausgaben aktivieren/deaktivieren. Warning-Logeinträge werden nicht ausgegeben.
	<input checked="" type="checkbox"/> Warning-Logausgaben aktivieren/deaktivieren. Warning-Logeinträge werden ausgegeben.
Info	<input type="checkbox"/> Info-Logausgaben aktivieren/deaktivieren. Info-Logeinträge werden nicht ausgegeben.
	<input checked="" type="checkbox"/> Info-Logausgaben aktivieren/deaktivieren. Info-Logeinträge werden ausgegeben.
Debug	<input type="checkbox"/> Debug-Logausgaben aktivieren/deaktivieren. Debug-Logeinträge werden nicht ausgegeben.
	<input checked="" type="checkbox"/> Debug-Logausgaben aktivieren/deaktivieren. Debug-Logeinträge werden ausgegeben.
[Submit]	Änderung übernehmen; Die Änderung wird erst nach dem nächsten Neustart des Controllers oder einem BACnet Restart wirksam.

### Gruppe „BACnet Network Capture“

Tabelle 201: WBM-Seite „BACnet Configuration“ – Gruppe „BACnet Network Capture“

Parameter	Bedeutung
Enable	<input type="checkbox"/> Aufzeichnung des Netzwerkverkehrs mit den entsprechenden BACnet Filtern aktivieren/deaktivieren. Netzwerkverkehr wird nicht aufgezeichnet.
	<input checked="" type="checkbox"/> Aufzeichnung des Netzwerkverkehrs mit den entsprechenden BACnet Filtern aktivieren/deaktivieren. Netzwerkverkehr wird aufgezeichnet.
Log pre-master secrets	<input type="checkbox"/> Speicherung der Secrets für die Entschlüsselung des BACnet/SC Netzwerkverkehrs aktivieren/deaktivieren. Secrets werden nicht gespeichert.
	<input checked="" type="checkbox"/> Speicherung der Secrets für die Entschlüsselung des BACnet/SC Netzwerkverkehrs aktivieren/deaktivieren. Secrets werden gespeichert.

Parameter	Bedeutung
[Submit]	Änderung übernehmen; Die Änderung wird erst nach dem nächsten Neustart des Controllers oder einem BACnet Restart wirksam.
BACnet Network Capture Archive [Download]	Über die Schaltfläche [Download] können Sie den aufgezeichneten Netzwerkverkehr incl. der Secrets, falls die Option aktiviert ist, vom Gerät herunterladen.

#### 7.1.1.4.4 Seite „BACnet Data Link“

##### Gruppe „Restart“

Tabelle 202: WBM-Seite „BACnet Data Link“ – Gruppe „BACnet Restart“

Parameter	Bedeutung
[Restart]	Neustart des BACnet Dienstes

##### Gruppe „BACnet/IP“

Tabelle 203: WBM-Seite „BACnet Data Link“ – Gruppe „BACnet/IP“

Parameter	Bedeutung
Port Number	Eingabe des Ports für die BACnet/IP Kommunikation
[Submit]	Änderung übernehmen; Die Änderung wird erst nach dem nächsten Neustart des Controllers oder einem BACnet Restart wirksam.

##### Gruppe „BACnet/SC“

Tabelle 204: WBM-Seite „BACnet Data Link“ – Gruppe „BACnet/SC“

Parameter	Bedeutung
Mode	Auswahl der BACnet/SC Betriebsart
	regular Das Gerät wird als BACnet/SC Node betrieben.
	primary Das Gerät wird als BACnet/SC Primary HUB betrieben.
	failover Das Gerät wird als BACnet/SC Failover HUB betrieben.
Port Number	Eingabe des Ports für die BACnet/SC Kommunikation
Primary Hub URI	Eingabe des URI für den Primary HUB; wss://<IP-Adresse>:<Port des HUBs> bzw. wss://<Domainname>:<Port des HUBs> (z. B. wss://192.168.178.19:47808 bzw. wss://PFC200V3-XXXXXX.localdomain.lan:47808)
Failover Hub URI	Eingabe des URI für den Failover HUB; wss://<IP-Adresse>:<Port des HUBs> bzw. wss://<Domainname>:<Port des HUBs> (z. B. wss://192.168.178.19:47808 bzw. wss://PFC200V3-XXXXXX.localdomain.lan:47808)
Allow self signed Certificates	Aktivieren/deaktivieren, ob die Kommunikation über selbstsignierte Zertifikate aufgebaut werden darf.
Allow expired Certificates	Aktivieren/deaktivieren, ob die Kommunikation über abgelaufene Zertifikate aufgebaut werden darf.
Allow any Certificates	Aktivieren/deaktivieren, ob die Kommunikation über beliebige Zertifikate aufgebaut werden darf.
[Submit]	Änderung übernehmen; Die Änderung wird erst nach dem nächsten Neustart des Controllers oder einem BACnet Restart wirksam.

### Gruppe „BACnet/SC Certificate Authority (CA)“

Tabelle 205: WBM-Seite „BACnet Data Link“ – Gruppe „BACnet/SC Certificate Authority (CA)“

Parameter	Bedeutung
Chose file ...	Auswahl des CA-Zertifikats auf dem Computer für die Übertragung auf das Gerät
[Upload]	Übertragung des ausgewählten CA-Zertifikats auf das Gerät; Nach dem Neustart wird dieses Zertifikat als CA-Zertifikat für die BACnet/SC Kommunikation verwendet.

### Gruppe „BACnet/SC Certificate“

Tabelle 206: WBM-Seite „BACnet Data Link“ – Gruppe „BACnet/SC Certificate“

Parameter	Bedeutung
Chose file ...	Auswahl des Gerätezertifikats auf dem Computer für die Übertragung zum Gerät
[Upload]	Übertragung des ausgewählten Gerätezertifikats auf das Gerät; Nach dem Neustart wird dieses Zertifikat für die BACnet/SC Kommunikation verwendet.

### Gruppe „BACnet/SC Certificate Signing Request (CSR)“

Tabelle 207: WBM-Seite „BACnet Configuration“ – Gruppe „BACnet/SC Certificate Signing Request (CSR)“

Parameter	Bedeutung
Country	Eingabe des Landes für den CSR bzw. für das Gerätezertifikat (zwei Buchstaben)
State	Eingabe des Staates für den CSR bzw. für das Gerätezertifikat
Locality	Eingabe des Ortes für den CSR bzw. für das Gerätezertifikat
Organization	Eingabe der Firma bzw. der Organisation für den CSR bzw. für das Gerätezertifikat
Organizational Unit	Eingabe der Abteilung für den CSR bzw. für das Gerätezertifikat
Common Name	Eingabe des Gerätenamens für den CSR bzw. für das Gerätezertifikat
[Generate]	Erstellung eines CSR sowie eines neuen privaten Schlüssels auf dem Gerät
[Download]	CSR vom Gerät herunterladen

### Gruppe „BACnet/SC Default Certificates“

Tabelle 208: WBM-Seite „BACnet Data Link“ – Gruppe „BACnet/SC Default Certificates“

Parameter	Bedeutung
[Generate]	Erstellung eines neuen Zertifikates

#### 7.1.1.4.5 Seite „BACnet Storage Location“

Auf der Seite „BACnet Storage Location“ können Sie Einstellungen für die Speicherung der BACnet spezifischen Parameter vornehmen.

### Gruppe „BACnet Persistence“

Tabelle 209: WBM-Seite „BACnet Storage Location“ – Gruppe „BACnet Persistence“

Parameter	Bedeutung	
Storage Location	Speicherort für die Persistenzdaten auswählen; Die Auswahl ist nur möglich, wenn beide Speicher vorhanden sind.	
	Internal Flash	Die Daten werden im internen Speicher des Controllers gespeichert.
	SD-Card	Die Daten werden auf der Speicherkarte gespeichert. Wenn „SD-Card“ ausgewählt ist, aber die Speicherkarte nicht mehr gesteckt ist, dann ist diese Option nicht mehr aktiv und nur noch „Internal Flash“ auswählbar.

Parameter	Bedeutung
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.

### Gruppe „BACnet Trendlog“

Tabelle 210: WBM-Seite „BACnet Storage Location“ – Gruppe „BACnet Trendlog“

Parameter	Bedeutung
Storage Location	Speicherort für die Trendlogdaten auswählen; Die Auswahl ist nur möglich, wenn beide Speicher vorhanden sind.
Internal Flash	Die Daten werden im internen Speicher des Controllers gespeichert.
SD-Card	Die Daten werden auf der Speicherkarte gespeichert. Wenn „SD-Card“ ausgewählt ist, aber die Speicherkarte nicht mehr gesteckt ist, dann ist diese Option nicht mehr aktiv und nur noch „Internal Flash“ auswählbar.
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.

### Gruppe „BACnet Eventlog“

Tabelle 211: WBM-Seite „BACnet Storage Location“ – Gruppe „BACnet Eventlog“

Parameter	Bedeutung
Storage Location	Speicherort für die Eventlogdaten auswählen; Die Auswahl ist nur möglich, wenn beide Speicher vorhanden sind.
Internal Flash	Die Daten werden im internen Speicher des Controllers gespeichert.
SD-Card	Die Daten werden auf der Speicherkarte gespeichert. Wenn „SD-Card“ ausgewählt ist, aber die Speicherkarte nicht mehr gesteckt ist, dann ist diese Option nicht mehr aktiv und nur noch „Internal Flash“ auswählbar.
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.

#### 7.1.1.4.6 Seite „BACnet Info“

Auf der Seite „BACnet Info“ finden Sie die Einstellungen zur Anzeige von BACnet spezifischen Informationen.

### Gruppe „Refresh Options“

Tabelle 212: WBM-Seite „BACnet Info“ – Gruppe „Refresh Options“

Parameter	Bedeutung
Automatic refresh interval (sec)	Zyklische Aktualisierung einschalten/ausschalten; Zykluszeit in Sekunden eingeben, mit der eine zyklische Aktualisierung durchgeführt wird; Abhängig vom Status wechselt die Beschriftung der Schaltfläche („Refresh“/„Start“/„Stop“).
[Refresh]	Anzeige aktualisieren; Die Schaltfläche ist nur sichtbar, wenn die zyklische Aktualisierung nicht eingeschaltet ist.
[Start]	Zyklische Aktualisierung starten; Die Schaltfläche ist nur sichtbar, wenn die zyklische Aktivierung eingeschaltet ist, aber noch nicht gestartet wurde.
[Stop]	Zyklische Aktualisierung beenden; Die Schaltfläche ist nur sichtbar, wenn die zyklische Aktualisierung aktiv ist.

Die zyklische Aktualisierung wird nur so lange durchgeführt, wie die Seite „BACnet Info“ geöffnet ist. Wenn Sie die WBM-Seite wechseln, wird die Aktualisierung angehalten, bis Sie die Seite „BACnet Info“ erneut aufrufen.

### Gruppe „BACnet/IP Statistics“

Tabelle 213: WBM-Seite „BACnet Info“ – Gruppe „BACnet/IP Statistics“

Parameter	Bedeutung
BACnet/IP Statistics	BACnet/IP Statistik Wenn keine Daten vorhanden sind, wird „no data available or retrieved“ angezeigt.

### Gruppe „BACnet/SC Statistics“

Tabelle 214: WBM-Seite „BACnet Info“ – Gruppe „BACnet/SC Statistics“

Parameter	Bedeutung
BACnet/SC Statistics	BACnet/SC Statistik Wenn keine Daten vorhanden sind, wird „no data available or retrieved“ angezeigt.

### BACnet/SC Connections“

Tabelle 215: WBM-Seite „BACnet Info“ – Gruppe „BACnet/SC Connections“

Parameter	Bedeutung
BACnet/SC Connections	BACnet/SC Verbindungen Wenn keine Daten vorhanden sind, wird „no data available or retrieved“ angezeigt.

## 7.1.1.5 Registerkarte „Security“

### 7.1.1.5.1 Seite „OpenVPN / IPsec“

#### Hinweis

#### Potentielle Sicherheitslücke bei VPN-Protokollen!

VPN-Protokolle bieten per Default die Möglichkeit, Hook-Scripte auszuführen. Das stellt eine potenzielle Sicherheitslücke dar.

1. Wenn Sie die Möglichkeit, Hook-Protokolle zu verwenden, nicht nutzen, schalten Sie diese in der Konfiguration ab. Passen Sie dazu die entsprechende Konfigurationsdatei an.
2. Um die Nutzung von Hook-Befehlen in OpenVPN abzuschalten, verwenden Sie in der Konfigurationsdatei „openvpn.conf“ den Befehl `--script-security level 1`. Weitere Informationen finden Sie unter [www.openvpn.net/community-resources/reference-manual-for-openvpn-2-5/#scripting-integration](http://www.openvpn.net/community-resources/reference-manual-for-openvpn-2-5/#scripting-integration).
3. Um die Nutzung von Hook-Befehlen in IPsec abzuschalten, verwenden Sie in der Konfigurationsdatei „ipsec.conf“ den Befehl `--disable-updown`. Weitere Informationen finden Sie unter [www.wiki.strogswan.org/projects/strongswan/wiki/Updown/](http://www.wiki.strogswan.org/projects/strongswan/wiki/Updown/).

Auf der Seite „OpenVPN / IPsec“ finden Sie die Einstellungen zu OpenVPN und IPsec.

### Gruppe „OpenVPN“

Tabelle 216: WBM-Seite „OpenVPN / IPsec“ – Gruppe „OpenVPN“

Parameter	Bedeutung	
Current State	Aktueller Status des OpenVPN-Dienstes	
	stopped	Der Dienst ist nicht aktiv.
	running	Der Dienst ist aktiv.
OpenVPN enabled	OpenVPN-Dienst aktivieren/deaktivieren	
openvpn.conf	OpenVPN-Konfigurationsdatei auswählen, die vom PC zum Produkt oder umgekehrt übertragen werden soll	
[Submit]	Änderung übernehmen; Die Änderung wird erst nach dem nächsten Neustart wirksam.	
Choose file ...	Datei auf dem Produkt oder PC auswählen	
[Upload]	Übertragen der ausgewählten Datei vom PC zum Produkt	
[Download]	Übertragen der ausgewählten Datei vom Produkt zum PC	

### Gruppe „IPsec“

Tabelle 217: WBM-Seite „OpenVPN / IPsec“ – Gruppe „IPsec“

Parameter	Bedeutung	
Current State	Aktueller Status des IPsec-Dienstes	
	stopped	Der Dienst ist nicht aktiv.
	running	Der Dienst ist aktiv.
IPsec enabled	IPsec-Dienst aktivieren/deaktivieren	
ipsec.conf	IPsec-Konfigurationsdatei auswählen, die vom PC zum Produkt oder umgekehrt übertragen werden soll	
ipsec.secrets	IPsec-Secrets-Datei auswählen, die vom PC zum Produkt oder umgekehrt übertragen werden soll	
[Submit]	Änderung übernehmen; Die Änderung wird erst nach dem nächsten Neustart wirksam.	
Choose file ...	Datei auf dem Produkt oder PC auswählen	
[Upload]	Übertragen der ausgewählten Datei vom PC zum Produkt	
[Download]	Übertragen der ausgewählten Datei vom Produkt zum PC	

#### 7.1.1.5.2 Seite „General Firewall Configuration“

Auf der Seite „General Firewall Configuration“ finden Sie die globalen Einstellungen zur Firewall.

#### Gruppe „Global Firewall Parameter“

Tabelle 218: WBM-Seite „General Firewall Configuration“ – Gruppe „Global Firewall Parameter“

Parameter	Bedeutung
Firewall enabled entirely	Komplette Funktionalität der Firewall aktivieren/deaktivieren Diese Einstellung hat oberste Priorität. Ist die Firewall ausgeschaltet, haben alle anderen Einstellungen keine direkte Auswirkung. Die Konfiguration der anderen Parameter ist trotzdem möglich, damit die Firewall-Parameter korrekt eingestellt werden können, bevor die Firewall aktiviert wird. Diese Einstellung ist unabhängig von der Einstellung zu „Filter enabled“ in der Gruppe „MAC address filter state Bridge <n>“ auf der Seite „MAC address filter state Bridge“.
ICMP echo broadcast protection	„ICMP echo broadcast“-Schutz aktivieren/deaktivieren
Max. UDP connections per second	Maximale Anzahl der UDP-Verbindungen pro Sekunde eingeben

Parameter	Bedeutung
Max. TCP connections per second	Maximale Anzahl der TCP-Verbindungen pro Sekunde eingeben
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.

### Hinweis

#### **CODESYS Dienste werden bei eingeschalteter Firewall ohne User-Filter abgewiesen!**

Wenn CODESYS Dienste (z. B. Modbus, OPC-UA, SNMP oder IIOT) genutzt werden, müssen in der Firewall-Konfiguration User-Filter für diese Dienste angelegt werden. Die User-Filter müssen so konfiguriert sein, dass die entsprechenden Ports akzeptiert werden.

#### 7.1.1.5.3 Seite „Interface Configuration“

Auf der Seite „Interface Configuration“ finden Sie die Firewall-Einstellungen zu den einzelnen Schnittstellen.

#### **Gruppe „Firewall Configuration Bridge <n> / VPN“**

Für jede konfigurierte Bridge wird eine eigene Gruppe angezeigt.

Die Einstellungen in dieser Gruppe beziehen sich auf die Konfiguration der Firewall auf IP-Niveau.

Tabelle 219: WBM-Seite „Interface Configuration“ – Gruppe „Firewall Configuration Bridge <n> / VPN / WAN“

Parameter	Bedeutung
Firewall enabled for Interface	Firewall für die jeweilige Schnittstelle aktivieren/deaktivieren
ICMP echo protection	„ICMP echo“-Schutz für die jeweilige Schnittstelle aktivieren/deaktivieren
ICMP echo limit per second	Maximale Anzahl „ICMP pings“ pro Sekunde eingeben. „0“ = „Disabled“
ICMP burst limit (0=disabled)	Maximale Anzahl „ICMP echo burst“ pro Sekunde eingeben
Service Configuration	Firewall für den jeweiligen Dienst aktivieren/deaktivieren
FTP/FTPES	Nicht jeder der hier gezeigten Dienste ist für jedes Produkt verfügbar.
FTPES (implicit)	Die Dienste selber müssen über die Seite „Ports and Services“ gesondert ein und ausgeschaltet werden.
HTTP	
HTTPS	
I/O Check	
PLC Runtime	
WebVisu – HTTP (port 8080)	
WebVisu – HTTPS (port 8081)	
SSH	
SNMP	
OPC UA (port 4840)	
BACnet (port 47808)	
PROFINET IO	
DNP3 (port 20000)	
IEC60870-5-104 (port 2404)	
IEC61850 (port 102)	
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.

Auf Controllern mit Telecontrol-Funktionalität werden standardmäßig die in der nachfolgenden Tabelle aufgelisteten Firewall-Ports geöffnet. Über diese Ports können die entsprechenden Telecontrol-Dienste ausgeführt werden, ohne dass deren Kommunikation durch die Firewall blockiert wird.

Tabelle 220: Ports für Telecontrol-Funktionalität

Protokoll	Port
DNP3	20000
IEC60870-5-104	2404
IEC61850	102

#### 7.1.1.5.4 Seite „Configuration of MAC address filter“

Auf dieser Seite stellen Sie die Firewall-Konfiguration auf ETHERNET-Niveau ein.

Die „MAC Address Filter Whitelist“ enthält zwei Default-Einträge mit folgenden Werten:

- Beschreibung: All WAGO devices  
MAC-Adresse: 00:30:DE:00:00:00  
MAC-Mask: ff:ff:ff:00:00:00
- Beschreibung: Enable docker bridges  
MAC-Adresse: 02:42:00:00:00:00  
MAC-Mask: ff:ff:00:00:00:00

Wenn Sie den ersten Default-Eintrag freischalten, können bereits verschiedene WAGO Produkte im Netzwerk untereinander kommunizieren.

#### Hinweis

##### **Vor Aktivierung des Filters MAC-Adresse freischalten!**

Bevor Sie den MAC-Adressenfilter aktivieren, müssen Sie Ihre eigene MAC-Adresse in der „MAC Address Filter Whitelist“ eintragen und freischalten. Andernfalls können Sie anschließend über das ETHERNET nicht mehr auf das Produkt zugreifen. Dies gilt auch für andere Dienste, die von Ihrem Produkt benutzt werden, z. B. die IP-Konfiguration über DHCP.

Wenn die MAC-Adresse Ihres DHCP-Servers nicht in der „MAC Address Filter Whitelist“ enthalten ist, wird Ihr Produkt nach dem nächsten Aktualisierungszyklus seine IP-Einstellungen verlieren und ist dann ebenfalls nicht mehr erreichbar.

Solange in der „MAC Address Filter Whitelist“ kein Eintrag enthalten ist, wird deshalb das Einschalten des Filters verhindert.

Falls mindestens eine freigeschaltete Adresse eingetragen ist, erhalten Sie vor dem Freischalten noch einmal einen dementsprechenden Warnhinweis, den Sie bestätigen müssen.

Die oben beschriebene Überprüfung wird nur im WBM, nicht aber im CBM durchgeführt!

#### **Gruppe „Global MAC address filter state“**

Tabelle 221: WBM-Seite „Configuration of MAC address filter“ – Gruppe „Global MAC address filter state“

Parameter	Bedeutung
Filter enabled	Globalen MAC-Adressenfilter aktivieren/deaktivieren
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.

#### **Gruppe „MAC address filter state Bridge <n>“**

Für jede konfigurierte Bridge wird eine eigene Gruppe angezeigt.

Tabelle 222: WBM-Seite „Configuration of MAC address filter“ – Gruppe „MAC address filter state Bridge &lt;n&gt;“

Parameter	Bedeutung
Filter enabled	MAC-Adressenfilter für die jeweilige Bridge aktivieren/deaktivieren; Diese Einstellung ist unabhängig von der Einstellung zu „Firewall enabled entirely“ in der Gruppe „Global Firewall Parameter“ auf der Seite „General Firewall Configuration“.
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.

### Gruppe „MAC address filter whitelist“

Tabelle 223: WBM-Seite „Configuration of MAC address filter“ – Gruppe „MAC address filter whitelist“

Parameter	Bedeutung
Description	Beschreibung der Geräte bzw. Bereiche, die bei generell aktivierter Firewall durch das Aktivieren des Filters freigeschaltet werden können. Die Beschreibung ist nur bei den initial in der Werkseinstellung vorhandenen Einträgen sichtbar.
MAC address	MAC-Adresse des Listeneintrags
MAC mask	MAC-Maske des Listeneintrags
Filter enabled	Filter für den Listeneintrag aktivieren/deaktivieren
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.
[Delete]	Ausgewählten Eintrag löschen; Die Schaltfläche ist nur sichtbar, wenn Einträge vorhanden sind.
[Add]	Neuen Eintrag hinzufügen.

#### 7.1.1.5.5 Seite „Configuration of User Filter“

Auf der Seite „Configuration of User Filter“ finden Sie die Einstellungen zu den anwenderspezifischen Filtern der Firewall.

#### Gruppe „User filter“

Für jeden konfigurierten Filter wird ein eigener Bereich angezeigt.

Tabelle 224: WBM-Seite „Configuration of User Filter“ – Gruppe „User filter“

Parameter	Bedeutung	
Policy	Netzwerkteilnehmer durch den Filter zulassen/ausschließen	
	Allow	Der Netzwerkteilnehmer ist zugelassen.
	Drop	Der Netzwerkteilnehmer ist ausgeschlossen.
Source IP address	Quell-IP-Adresse für den Filter	
Source Netmask	Quellnetzmaske für den Filter	
Source Port	Quell-Port-Nummer für den Filter	
Destination IP address	Ziel-IP-Adresse für den Filter	
Destination Netmask	Zielnetzmaske für den Filter	
Destination Port	Ziel-Port-Nummer für den Filter	
Protocol	Protokolle für den Filter	
	TCP/UDP	Der TCP-Service und der UDP-Service werden gefiltert.
	TCP	Der TCP-Service wird gefiltert.
	UDP	Der UDP-Service wird gefiltert.
Input Interface	Schnittstellen für den Filter	
	Any	Alle Schnittstellen werden gefiltert.

Parameter	Bedeutung	
	Bridge <n>	Die zur Bridge <n> zugeordneten Schnittstellen werden gefiltert. Es werden nur die konfigurierten Bridges angezeigt.
	VPN	Die VPN-Schnittstelle wird gefiltert.
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.	

### **i Hinweis**

#### **CODESYS Dienste werden bei eingeschalteter Firewall ohne User-Filter abgewiesen!**

Wenn CODESYS Dienste (z. B. Modbus, OPC-UA, SNMP oder IIOT) genutzt werden, müssen in der Firewall-Konfiguration User-Filter für diese Dienste angelegt werden. Die User-Filter müssen so konfiguriert sein, dass die entsprechenden Ports akzeptiert werden.

#### **7.1.1.5.6 Seite „Certificates“**

Auf dieser Seite finden Sie die Einstellungen zu den Zertifikaten.

#### **Gruppe „Installed Certificates“**

Tabelle 225: WBM-Seite „Certificates“ – Gruppe „Installed Certificates“

Parameter	Bedeutung
<certificate name>	Geladene Zertifikate; Wenn kein Zertifikat geladen wurde, wird „No certificates existing“ angezeigt.
[Delete]	Ausgewählten Eintrag löschen; Die Schaltfläche ist nur sichtbar, wenn Einträge vorhanden sind.
Choose file ...	Datei auf dem PC auswählen
[Upload]	Übertragen der ausgewählten Datei vom PC zum Produkt

Die Zertifikate werden im Verzeichnis „/etc/certificates/“ gespeichert.

#### **Gruppe „Installed Private Keys“**

Tabelle 226: WBM-Seite „Certificates“ – Gruppe „Installed Private Keys“

Parameter	Bedeutung
<private key name>	Geladenen Schlüssel; Wenn kein Schlüssel geladen wurde, wird „No private keys existing“ angezeigt.
[Delete]	Ausgewählten Eintrag löschen; Die Schaltfläche ist nur sichtbar, wenn Einträge vorhanden sind.
Choose file ...	Datei auf dem PC auswählen
[Upload]	Übertragen der ausgewählten Datei vom PC zum Produkt

Die Schlüssel werden im Verzeichnis „/etc/certificates/keys/“ gespeichert.

#### **7.1.1.5.7 Seite „Boot Mode Configuration“**

Auf der Seite „Boot mode configuration“ finden Sie Einstellungen zur Boot-Option.

### **i Hinweis**

**Wenn Sie das Booten vom internen Flash erzwingen, kann das Gerät nicht mehr über die Speicherkarte gestartet werden!**

Wenn aufgrund von Problemen oder falscher Konfiguration keine Verbindung mehr über ETHERNET möglich ist, haben sie die Möglichkeit, das Produkt über die Service-Schnittstelle und „WAGO Ethernet Settings“ wieder erreichbar zu machen.

#### **Gruppe „Force internal boot“**

Tabelle 227: WBM-Seite „Boot mode configuration“ – Gruppe „Force internal boot“

Parameter	Bedeutung	
Boot mode	Boot-Option für das Produkt einstellen	
	Memory card or internal flash	Booten ist vom internen Flash oder von der Speicherkarte möglich.
	Internal flash only	Booten ist nur vom internen Flash möglich.
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.	

#### **7.1.1.5.8 Seite „Security Settings“**

Auf dieser Seite finden Sie Einstellungen zur Netzwerksicherheit.

#### **Gruppe „TLS Configuration“**

Tabelle 228: WBM-Seite „Security Settings“ – Gruppe „TLS Configuration“

Parameter	Bedeutung	
TLS Configuration	Erlaubte TLS-Versionen und kryptografischen Verfahren für HTTPS einstellen	
	Extended Compatibility	Der Webserver erlaubt TLS 1.3 und auch TLS 1.2 mit weniger starken kryptografischen Verfahren.
	Strong	Der Webserver erlaubt nur TLS 1.3 und starke Algorithmen.
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.	

### **i Hinweis**

#### **Technische Richtlinie TR-02102 des BSI**

Die Regeln für die TLS-Einstellungen richten sich nach der technischen Richtlinie TR-02102 des Bundesamtes für Sicherheit in der Informationstechnik.

Die Richtlinie finden Sie unter: [www.bsi.bund.de](https://www.bsi.bund.de).

#### **7.1.1.5.9 Seite „Advanced Intrusion Detection Environment (AIDE)“**

Auf der Seite „Advanced Intrusion Detection Environment (AIDE)“ finden Sie Einstellungen zur Netzwerksicherheit.

#### **Gruppe „Run AIDE check at startup“**

Tabelle 229: WBM-Seite „Advanced Intrusion Detection Environment (AIDE)“ – Gruppe „Run AIDE check at startup“

Parameter	Bedeutung
Service active	„AIDE check“ beim Start des Controllers aktivieren/deaktivieren.

Parameter	Bedeutung	
	<input type="checkbox"/>	„AIDE check“ ist beim Start nicht aktiv.
	<input checked="" type="checkbox"/>	„AIDE check“ ist beim Start aktiv.
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.	

### Gruppe „Control AIDE and show log“

Tabelle 230: WBM-Seite „Advanced Intrusion Detection Environment (AIDE)“ – Gruppe „Control AIDE and show log“

Parameter	Bedeutung	
Select Action	Auszuführende Aktion auswählen.	
	readlog	Die Log-Daten werden angezeigt.
	init	Die Datenbank wird initialisiert und mit den aktuellen Werten gefüllt.
	check	Die aktuellen Werte werden mit den in der Datenbank gespeicherten Werten verglichen.
	update	Die aktuellen Werte werden mit den in der Datenbank gespeicherten Werten verglichen und die Datenbank anschließend aktualisiert.
Read only the last n	Anzeige der letzten n Meldungen einschalten/ausschalten; Anzahl der angezeigten Meldungen eingeben.	
Automatic refresh interval (sec)	Zyklische Aktualisierung einschalten/ausschalten; Zykluszeit in Sekunden eingeben, mit der eine zyklische Aktualisierung durchgeführt wird; Abhängig vom Status wechselt die Beschriftung der Schaltfläche („Refresh“/„Start“/„Stop“).	
[Refresh]	Anzeige aktualisieren; Die Schaltfläche ist nur sichtbar, wenn die zyklische Aktualisierung nicht eingeschaltet ist.	
[Start]	Zyklische Aktualisierung starten; Die Schaltfläche ist nur sichtbar, wenn die zyklische Aktivierung eingeschaltet ist, aber noch nicht gestartet wurde.	
[Stop]	Zyklische Aktualisierung beenden; Die Schaltfläche ist nur sichtbar, wenn die zyklische Aktualisierung aktiv ist.	

Die zyklische Aktualisierung wird nur so lange durchgeführt, wie die Seite „Advanced Intrusion Detection Environment (AIDE)“ geöffnet ist. Wenn Sie die WBM-Seite wechseln, wird die Aktualisierung angehalten, bis Sie die Seite „Advanced Intrusion Detection Environment (AIDE)“ erneut aufrufen.

Die Meldungen werden unterhalb der Einstellungen angezeigt.

#### 7.1.1.5.10 Seite „WAGO Device Access“

Auf der Seite „WAGO Device Access“ finden Sie Einstellungen zur Authentifizierung beim Scannen des Knotens.

#### Hinweis

##### Beta-Status

In der vorliegenden Firmwareversion befindet sich die „WAGODevice Access“-Funktionalität noch im Beta-Status!

## Gruppe „Unauthenticated Requests“

Tabelle 231: WBM-Seite „WAGO Device Access“ – Gruppe „Unauthenticated Requests“

Parameter	Bedeutung
Allow unauthenticated Device Scan	Hier stellen Sie ein, ob das Scannen des Knotens ohne Authentifizierung möglich ist. In der Default-Einstellung ist die Authentifizierung ausgeschaltet. Zur Erhöhung des Security-Levels können Sie die Authentifizierung für das Scannen des Knotens erzwingen. Im aktuellen Beta-Status werden beim Scannen nur Kopfstationen, aber keine I/O-Module erkannt!
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.

## Gruppe „CORS Configuration“

Tabelle 232: WBM-Seite „WAGO Device Access“ – Gruppe „CORS Configuration“

Parameter	Bedeutung	
CORS Policy	Auswählen, von welchen Origins „Cross Origin“-Zugriffe auf die REST-API durchgeführt werden dürfen.	
	Allow all	Von allen Origins dürfen „Cross Origin“-Zugriffe auf die REST-API durchgeführt werden.
	Allow all origins and null	Zusätzlich zu allen normalen Origins ist auch „null“ als Wert erlaubt, was manche Browser verwenden, um zu kennzeichnen, dass die Webseite von einem lokalen Dateisystem gehostet wird.
	Allow origins from whitelist	Es soll nur von den Origins auf die REST-API zugegriffen werden, die in der Whitelist erfasst sind. Achtung: Bei dieser Einstellung ist es zwingend erforderlich, dass die Origin Ihrer Anwendung in die Whitelist eingetragen wird, sonst wird der Browser den Zugriff auf die REST-API verhindern.
None	Der Webserver weist den Browser an, gar keine „Cross Origin“-Zugriffe durchzuführen.	
CORS Whitelist	Origins der Anwendungen eintragen, die einen „Cross Origin“-Zugriff auf die REST-API durchführen dürfen. Dieses Eingabefeld ist nur wirksam, wenn als „CORS Policy“-Wert „Allow origins from whitelist“ markiert ist.	
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.	

### 7.1.1.6 Registerkarte „Diagnostic“

#### 7.1.1.6.1 Seite „Log Message Viewer“

Auf der Seite „Log Message Viewer“ finden Sie die Einstellungen zur Anzeige der Diagnosemeldungen.

Tabelle 233: WBM-Seite „Log Message Viewer“ – Gruppe „Refresh Options“

Parameter	Bedeutung
Read only the last	Anzeige der letzten n Meldungen einschalten/ausschalten; Anzahl der angezeigten Meldungen eingeben
Automatic refresh interval (sec)	Zyklische Aktualisierung einschalten/ausschalten; Zykluszeit in Sekunden eingeben, mit der eine zyklische Aktualisierung durchgeführt wird; Abhängig vom Status wechselt die Beschriftung der Schaltfläche („Refresh“/„Start“/„Stop“).

Parameter	Bedeutung	
Source	Quelle der Diagnosemeldungen auswählen; Die Drop-Down-Liste ist abhängig vom angemeldeten Benutzer.	
	user	Nur Standard-Diagnosemeldungen
	admin	Standard-Diagnosemeldungen und alle Log-Dateien im Ordner <code>/var/log/*</code>
[Refresh]	Anzeige aktualisieren; Die Schaltfläche ist nur sichtbar, wenn die zyklische Aktualisierung nicht eingeschaltet ist.	
[Start]	Zyklische Aktualisierung starten; Die Schaltfläche ist nur sichtbar, wenn die zyklische Aktivierung eingeschaltet ist, aber noch nicht gestartet wurde.	
[Stop]	Zyklische Aktualisierung beenden; Die Schaltfläche ist nur sichtbar, wenn die zyklische Aktualisierung aktiv ist.	

Die zyklische Aktualisierung wird nur so lange durchgeführt, wie die Seite „Diagnostic Information“ geöffnet ist. Wenn Sie die WBM-Seite wechseln, wird die Aktualisierung angehalten, bis Sie die Seite „Diagnostic“ erneut aufrufen.

Die Meldungen werden unterhalb der Einstellungen angezeigt.

#### 7.1.1.6.2 Seite „Download“

Auf der Seite „Download“ haben Sie die Möglichkeit, Diagnosedaten vom Produkt herunterzuladen.

Tabelle 234: WBM-Seite „Download“ – Gruppe „Diagnostic Information“

Parameter	Bedeutung
[Download]	Diagnoseinformationen vom Gerät herunterladen

Die erstellte Archivdatei enthält die Log-Nachrichten, die Firmwareversion und eine Liste mit den installierten Paketen.

#### 7.1.1.6.3 Seite „Network Capture“

Auf der Seite „Network Capture“ finden Sie die notwendigen Einstellungen, um den Netzwerkverkehr auf dem Gerät aufzeichnen und herunterladen zu können. Der aktuelle Status der Netzwerkaufzeichnung wird angezeigt.

##### Gruppe „State“

Tabelle 235: WBM-Seite „Network Capture“ – Gruppe „State“

Parameter	Bedeutung
Current State	Aktueller Status der Netzwerkaufzeichnung
Last Captured Package Count	Bereits aufgezeichnete Netzwerkpakete
Last Refresh Time	Zeitpunkt der letzten Aktualisierung von „Current State“ und „Last Captured Package Count“

##### Gruppe „Configuration“

Tabelle 236: WBM-Seite „Network Capture“ – Gruppe „Configuration“

Parameter	Bedeutung
Enable	Aufzeichnung einschalten/ausschalten

Parameter	Bedeutung			
Rotate Log Files	Rotierendes Aufzeichnen einschalten/ausschalten; Wenn diese Option eingeschaltet ist, wird der Netzwerkverkehr in bis zu drei Dateien mit der eingestellten maximalen Dateigröße abgespeichert. Ist die maximale Dateigröße der ersten Datei erreicht, werden die Daten in einer zweiten Datei weiter aufgezeichnet usw. Ist auch die maximale Dateigröße der dritten Datei erreicht, werden die Daten der ersten Datei überschrieben.			
Max. Filesize	Maximale Dateigröße für die Datenaufzeichnung eingeben			
Storage Location	Speicherort für die aufgezeichneten Daten auswählen			
	<table border="1"> <tr> <td>Internal Flash</td> <td>Die Daten werden im internen Speicher gespeichert.</td> </tr> <tr> <td>SD-Card</td> <td>Die Daten werden auf der Speicherkarte gespeichert. Wenn „SD-Card“ ausgewählt ist, aber die Speicherkarte nicht mehr gesteckt ist, dann ist diese Option nicht mehr aktiv und nur noch „Internal-Flash“ auswählbar.</td> </tr> </table>	Internal Flash	Die Daten werden im internen Speicher gespeichert.	SD-Card
Internal Flash	Die Daten werden im internen Speicher gespeichert.			
SD-Card	Die Daten werden auf der Speicherkarte gespeichert. Wenn „SD-Card“ ausgewählt ist, aber die Speicherkarte nicht mehr gesteckt ist, dann ist diese Option nicht mehr aktiv und nur noch „Internal-Flash“ auswählbar.			
Listen On Network Interface	Netzwerkinterface auswählen, von welchem der Netzwerkverkehr mitgeschnitten werden soll; Zur Auswahl stehen dabei die verfügbaren Netzwerkschnittstellen des Gerätes.			
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.			

### Gruppe „Filter Configuration“

Tabelle 237: WBM-Seite „Network Capture“ – Gruppe „Filter Configuration“

Parameter	Bedeutung
Capture Filter	Aufzeichnungsfiler eingegeben; Diese dienen dazu, nur den relevanten bzw. gewünschten Datenverkehr mitzuschneiden. So ist es bspw. möglich, nur die Kommunikation von nur einem Port aufzuzeichnen oder von einer bestimmten IP-Adresse. Weitere Informationen zu den möglichen Filtereinstellungen finden Sie in den Erläuterungen der „Capture Filter“ in der Dokumentation zu „Wireshark“.
[Check]	Eingegebenen „Capture Filter“ auf Korrektheit überprüfen
[Submit]	Änderung übernehmen; Die Änderung wird sofort wirksam.

### Gruppe „Log Download“

Tabelle 238: WBM-Seite „Network Capture“ – Gruppe „Log Download“

Parameter	Bedeutung
Select Log File	Mitschnitt auswählen, der vom Produkt heruntergeladen werden soll
[Download]	Ausgewählten Mitschnitt vom Produkt herunterladen
[Download All]	Alle vorhandenen Mitschnitte vom Produkt herunterladen

# Tabellenverzeichnis

Tabelle 1	WBM-Seite „Device Status“ – Gruppe „Device Details“ .....	14
Tabelle 2	WBM-Seite „Device Status“ – Gruppe „Network TCP/IP Details“ .....	14
Tabelle 3	WBM-Seite „PLC Runtime Information“ – Gruppe „Runtime“ .....	15
Tabelle 4	WBM-Seite „Clock“ – Gruppe „Timezone and Format“ .....	15
Tabelle 5	WBM-Seite „Configuration of NTP Client“ – Gruppe „NTP Client Configuration“ .....	15
Tabelle 6	CODESYS V3-Prioritäten.....	17
Tabelle 7	WBM-Seite „PLC Runtime Configuration“ – Gruppe „General PLC Runtime Configuration“ ...	17
Tabelle 8	WBM-Seite „PLC Runtime Configuration“ – Gruppe „Webserver Configuration“ .....	18
Tabelle 9	WBM-Seite „PLC Runtime Services“ – Gruppe „CODESYS V3“ .....	18
Tabelle 10	WBM-Seite „Controls Settings“ – Gruppe „OMS Controls“ .....	19
Tabelle 11	WBM-Seite „Configuration of Serial Interface“ – Gruppe „Current Serial Interface Configuration“ .....	21
Tabelle 12	WBM-Seite „Configuration of Serial Interface“ – Gruppe „Assign Owner of Serial Interface“	21
Tabelle 13	WBM-Seite „Configuration of Serial Interface“ – Gruppe „Assign Mode of Serial Interface“ .	22
Tabelle 14	WBM-Seite „Configuration of Serial Interface“ – Gruppe „Current Serial Interface Configuration“ .....	22
Tabelle 15	WBM-Seite „Configuration of Serial Interface“ – Gruppe „Bus Termination“ .....	23
Tabelle 16	WBM-Seite „Configuration of Serial Interface“ – Gruppe „Bias Network“ .....	23
Tabelle 17	WBM-Seite „Configuration of Service Interface“ – Gruppe „Assign Owner of Service Interface“ .....	23
Tabelle 18	WBM-Seite „Ethernet Configuration“ – Gruppe „Bridge Configuration“ .....	25
Tabelle 19	WBM-Seite „Ethernet Configuration“ – Gruppe „Dummy Interfaces“ .....	25
Tabelle 20	WBM-Seite „Ethernet Configuration“ – Gruppe „VLAN Interfaces“ .....	25
Tabelle 21	WBM-Seite „Ethernet Configuration“ – Gruppe „Port Mirror Settings“ .....	25
Tabelle 22	WBM-Seite „Ethernet Configuration“ – Gruppe „Storm Control Settings“ .....	26
Tabelle 23	WBM-Seite „Ethernet Configuration“ – Gruppe „Storm Control Settings“ .....	26
Tabelle 24	WBM-Seite „Ethernet Configuration“ – Gruppe „Storm Control Settings“ .....	26
Tabelle 25	WBM-Seite „Ethernet Configuration“ – Gruppen „Ethernet Interface Configuration“ .....	26
Tabelle 26	WBM-Seite „Ethernet Configuration“ – Gruppen „Ethernet Interface Configuration“ .....	27
Tabelle 27	WBM-Seite „TCP/IP Configuration“ – Gruppe „Bridge Interfaces“ .....	27
Tabelle 28	WBM-Seite „TCP/IP Configuration“ – Gruppe „Dummy Interfaces“ .....	28
Tabelle 29	WBM-Seite „TCP/IP Configuration“ – Gruppe „VLAN Interfaces“ .....	28
Tabelle 30	WBM-Seite „TCP/IP Configuration“ – Gruppe „DNS Server“ .....	29
Tabelle 31	WBM-Seite „Configuration of Host- and Domain Name“ – Gruppe „Hostname“ .....	29
Tabelle 32	WBM-Seite „Configuration of Host- and Domain Name“ – Gruppe „Domain Name“ .....	30
Tabelle 33	WBM-Seite „Routing“ – Gruppe „IP Forwarding through multiple interfaces“ .....	30
Tabelle 34	WBM-Seite „Routing“ – Gruppe „Custom Routes“ .....	32

Tabelle 35	WBM-Seite „Routing“ – Gruppe „Dynamic Routes (assigned by DHCP)“ .....	33
Tabelle 36	WBM-Seite „Routing“ – Gruppe „IP Masquerading“ .....	34
Tabelle 37	WBM-Seite „Routing“ – Gruppe „Port Forwarding“ .....	34
Tabelle 38	Dienste und Benutzer .....	35
Tabelle 39	Linux <sup>®</sup> -Benutzer .....	35
Tabelle 40	WBM-Seite „WBM User Configuration“ – Gruppe „Change Passwords“ .....	36
Tabelle 41	WBM-Seite „Security Settings“ – Gruppe „TLS Configuration“ .....	37
Tabelle 42	WBM-Seite „General Firewall Configuration“ – Gruppe „Global Firewall Parameter“ .....	38
Tabelle 43	WBM-Seite „Interface Configuration“ – Gruppe „Firewall Configuration Bridge <n> / VPN / WAN“ .....	38
Tabelle 44	Ports für Telecontrol-Funktionalität.....	39
Tabelle 45	WBM-Seite „Configuration of MAC address filter“ – Gruppe „Global MAC address filter state“ .....	39
Tabelle 46	WBM-Seite „Configuration of MAC address filter“ – Gruppe „MAC address filter state Bridge <n>“ .....	39
Tabelle 47	WBM-Seite „Configuration of MAC address filter“ – Gruppe „MAC address filter whitelist“ .....	40
Tabelle 48	WBM-Seite „Configuration of User Filter“ – Gruppe „User filter“ .....	40
Tabelle 49	Liste der per DHCP übertragenen Parameter .....	42
Tabelle 50	WBM-Seite „DHCP Server Configuration“ – Gruppe „DHCP Server Configuration Bridge <n>“ .....	42
Tabelle 51	WBM-Seite „Configuration of DNS Server“ – Gruppe „DNS Server“ .....	43
Tabelle 52	WBM-Seite „Configuration of general SNMP parameters“ – Gruppe „General SNMP Configuration“ .....	44
Tabelle 53	WBM-Seite „Configuration of SNMP v1/v2c Parameters“ – Gruppe „Communities“ .....	44
Tabelle 54	WBM-Seite „Configuration of SNMP v1/v2cparameters“ – Gruppe „Trap Receivers“ .....	45
Tabelle 55	WBM-Seite „Configuration of SNMP v3 Parameters“ – Gruppe „Users“ .....	45
Tabelle 56	WBM-Seite „Configuration of SNMP v3 Parameters“ – Gruppe „Trap Receivers“ .....	46
Tabelle 57	WBM-Seite „Configuration of Network Services“ – Gruppe „FTP“ .....	46
Tabelle 58	WBM-Seite „Configuration of Network Services“ – Gruppe „FTPES (explicit FTPS)“ .....	47
Tabelle 59	WBM-Seite „Configuration of Network Services“ – Gruppe „HTTP“ .....	47
Tabelle 60	WBM-Seite „Configuration of Network Services“ – Gruppe „HTTPS“ .....	47
Tabelle 61	WBM-Seite „Configuration of Network Services“ – Gruppe „I/O-CHECK“ .....	48
Tabelle 62	WBM-Seite „SSH Server Settings“ – Gruppe „SSH Server“ .....	48
Tabelle 63	WBM-Seite „Docker Settings“ – Gruppe „Docker Status“ .....	48
Tabelle 64	Komponenten des Softwarepaketes Cloud-Connectivity .....	49
Tabelle 65	WBM-Seite „Overview“ – Gruppe „Connection <n>“ .....	50
Tabelle 66	WBM-Seite „Configuration of Connection <n>“ – Gruppe „Configuration“ .....	50
Tabelle 67	Anzeige der Auswahl- und Eingabefelder abhängig von der ausgewählten Cloud-Plattform.	51
Tabelle 68	Auswahlmöglichkeit des Datenprotokolls abhängig von der ausgewählten Cloud-Plattform	53

Tabelle 69	Anzeige der Auswahl- und Eingabefelder abhängig vom ausgewählten Datenprotokoll.....	53
Tabelle 70	Auswahlmöglichkeit des Cache-Modes abhängig vom ausgewählten Datenprotokoll .....	53
Tabelle 71	Anzeige der Eingabefelder abhängig von der ausgewählten Authentifizierung .....	53
Tabelle 72	WBM-Seite „OPC UA Configuration“ – Gruppe „OPC UA Server Configuration“ .....	54
Tabelle 73	WBM-Seite „OPC UA Configuration“ – Gruppe „OPC UA Server Security Settings“ .....	54
Tabelle 74	WBM-Seite „BACnet Status“ – Gruppe „BACnet Information“ .....	55
Tabelle 75	WBM-Seite „BACnet Status“ – Gruppe „BACnet License“ .....	55
Tabelle 76	WBM-Seite „BACnet Status“ – Gruppe „BACnet Data Link“ .....	55
Tabelle 77	WBM-Seite „BACnet Configuration“ – Gruppe „PLC Runtime“ .....	56
Tabelle 78	WBM-Seite „BACnet Configuration“ – Gruppe „BACnet Service“ .....	56
Tabelle 79	WBM-Seite „BACnet Configuration“ – Gruppe „BACnet Data“ .....	56
Tabelle 80	WBM-Seite „BACnet Configuration“ – Gruppe „BACnet Log Level“ .....	56
Tabelle 81	WBM-Seite „BACnet Configuration“ – Gruppe „BACnet Network Capture“ .....	57
Tabelle 82	WBM-Seite „BACnet Data Link“ – Gruppe „BACnet Restart“ .....	57
Tabelle 83	WBM-Seite „BACnet Data Link“ – Gruppe „BACnet/IP“ .....	57
Tabelle 84	WBM-Seite „BACnet Data Link“ – Gruppe „BACnet/SC“ .....	57
Tabelle 85	WBM-Seite „BACnet Data Link“ – Gruppe „BACnet/SC Certificate Authority (CA)“ .....	58
Tabelle 86	WBM-Seite „BACnet Data Link“ – Gruppe „BACnet/SC Certificate“ .....	58
Tabelle 87	WBM-Seite „BACnet Configuration“ – Gruppe „BACnet/SC Certificate Signing Request (CSR)“ .....	58
Tabelle 88	WBM-Seite „BACnet Data Link“ – Gruppe „BACnet/SC Default Certificates“ .....	58
Tabelle 89	WBM-Seite „BACnet Storage Location“ – Gruppe „BACnet Persistence“ .....	59
Tabelle 90	WBM-Seite „BACnet Storage Location“ – Gruppe „BACnet Trendlog“ .....	59
Tabelle 91	WBM-Seite „BACnet Storage Location“ – Gruppe „BACnet Eventlog“ .....	59
Tabelle 92	Übersicht über die Adressen im Objektverzeichnis.....	60
Tabelle 93	Indizierung der „IEC 61131-3“-Variablendaten im Objektverzeichnis.....	65
Tabelle 94	Feldbuszugriff auf die PFC-Ausgangsdaten .....	66
Tabelle 95	Beispiele für den CODESYS Zugriff auf PFC-Variablen .....	67
Tabelle 96	Maximale Indizes und Sub-Indizes für „IEC 61131-3“-Variablen .....	67
Tabelle 97	Beispiel für „IEC 61131-3“-Ausgangsvariablen.....	68
Tabelle 98	WBM-Seite „Firmware Backup“ – Gruppe „Firmware Backup“ .....	70
Tabelle 99	WBM-Seite „Firmware Restore“ – Gruppe „Firmware Restore“ .....	72
Tabelle 100	Laden eines Boot-Projekts .....	74
Tabelle 101	Übersicht Fehlercodes LED "I/O" .....	75
Tabelle 102	Fehlercode 1 - Hardware- und Konfigurationsfehler: Bedeutung der Blinkcodes und Maßnahmen zur Fehlerbehebung.....	76
Tabelle 103	Fehlercode 2 - Konfigurationsfehler: Bedeutung der Blinkcodes und Maßnahmen zur Fehlerbehebung .....	77

Tabelle 104	Fehlercode 3 - Lokalbus-Protokollfehler: Bedeutung der Blinkcodes und Maßnahmen zur Fehlerbehebung.....	77
Tabelle 105	Fehlercode 4 - Physischer Fehler am Lokalbus: Bedeutung der Blinkcodes und Maßnahmen zur Fehlerbehebung .....	78
Tabelle 106	Fehlercode 5 - Lokalbus-Initialisierungsfehler: Bedeutung der Blinkcodes und Maßnahmen zur Fehlerbehebung .....	78
Tabelle 107	Fehlercode 7 - Nicht unterstütztes I/O-Modul: Bedeutung der Blinkcodes und Maßnahmen zur Fehlerbehebung .....	78
Tabelle 108	Fehlercode 9 - CPU-Ausnahmefehler: Bedeutung der Blinkcodes und Maßnahmen zur Fehlerbehebung .....	78
Tabelle 109	Übersicht Fehlercodes LED "MS" .....	79
Tabelle 110	Fehlercode 1 - Konfigurationsfehler: Bedeutung der Blinkcodes und Maßnahmen zur Fehlerbehebung .....	79
Tabelle 111	WBM-Seite „Log Message Viewer“ – Gruppe „Refresh Options“ .....	79
Tabelle 112	WBM-Seite „Download“ – Gruppe „Diagnostic Information“ .....	79
Tabelle 113	WBM-Seite „Network Capture“ – Gruppe „State“ .....	79
Tabelle 114	WBM-Seite „Network Capture“ – Gruppe „Configuration“ .....	80
Tabelle 115	WBM-Seite „Network Capture“ – Gruppe „Filter Configuration“ .....	80
Tabelle 116	WBM-Seite „Network Capture“ – Gruppe „Log Download“ .....	80
Tabelle 117	Voreingestellte IP-Adressierung der ETHERNET-Schnittstellen.....	82
Tabelle 118	Netzmaske 255.255.255.0.....	82
Tabelle 119	Adresswahlschalter .....	85
Tabelle 120	Zugriffsrechte für die WBM-Seiten .....	91
Tabelle 121	Zugriffsrechte für die WBM-Seiten .....	102
Tabelle 122	WBM-Seite „Device Status“ – Gruppe „Device Details“ .....	104
Tabelle 123	WBM-Seite „Device Status“ – Gruppe „Network TCP/IP Details“ .....	104
Tabelle 124	WBM-Seite „PLC Runtime Information“ – Gruppe „Runtime“ .....	105
Tabelle 125	WBM-Seite „PLC Runtime Configuration“ – Gruppe „General PLC Runtime Configuration“ ...	106
Tabelle 126	WBM-Seite „PLC Runtime Configuration“ – Gruppe „Webserver Configuration“ .....	106
Tabelle 127	WBM-Seite „TCP/IP Configuration“ – Gruppe „Bridge Interfaces“ .....	107
Tabelle 128	WBM-Seite „TCP/IP Configuration“ – Gruppe „Dummy Interfaces“ .....	107
Tabelle 129	WBM-Seite „TCP/IP Configuration“ – Gruppe „VLAN Interfaces“ .....	108
Tabelle 130	WBM-Seite „TCP/IP Configuration“ – Gruppe „DNS Server“ .....	108
Tabelle 131	WBM-Seite „Ethernet Configuration“ – Gruppe „Bridge Configuration“ .....	109
Tabelle 132	WBM-Seite „Ethernet Configuration“ – Gruppe „Dummy Interfaces“ .....	109
Tabelle 133	WBM-Seite „Ethernet Configuration“ – Gruppe „VLAN Interfaces“ .....	109
Tabelle 134	WBM-Seite „Ethernet Configuration“ – Gruppe „Port Mirror Settings“ .....	109
Tabelle 135	WBM-Seite „Ethernet Configuration“ – Gruppe „Storm Control Settings“.....	110
Tabelle 136	WBM-Seite „Ethernet Configuration“ – Gruppe „Storm Control Settings“.....	110

Tabelle 137	WBM-Seite „Ethernet Configuration“ – Gruppe „Storm Control Settings“ .....	110
Tabelle 138	WBM-Seite „Ethernet Configuration“ – Gruppen „Ethernet Interface Configuration“ .....	110
Tabelle 139	WBM-Seite „Ethernet Configuration“ – Gruppen „Ethernet Interface Configuration“ .....	111
Tabelle 140	WBM-Seite „Configuration of Host- and Domain Name“ – Gruppe „Hostname“ .....	112
Tabelle 141	WBM-Seite „Configuration of Host- and Domain Name“ – Gruppe „Domain Name“ .....	112
Tabelle 142	WBM-Seite „Routing“ – Gruppe „IP Forwarding through multiple interfaces“ .....	112
Tabelle 143	WBM-Seite „Routing“ – Gruppe „Custom Routes“ .....	113
Tabelle 144	WBM-Seite „Routing“ – Gruppe „IP Masquerading“ .....	113
Tabelle 145	WBM-Seite „Routing“ – Gruppe „Port Forwarding“ .....	114
Tabelle 146	WBM-Seite „Spanning Tree Protocol“ – Gruppe „Status“ .....	115
Tabelle 147	WBM-Seite „Spanning Tree Protocol“ – Gruppe „Parameter Settings“ .....	116
Tabelle 148	WBM-Seite „Clock“ – Gruppe „Timezone and Format“ .....	117
Tabelle 149	WBM-Seite „Clock“ – Gruppe „UTC Time and Date“ .....	117
Tabelle 150	WBM-Seite „Clock“ – Gruppe „Local Time and Date“ .....	117
Tabelle 151	WBM-Seite „Configuration of Serial Interface“ – Gruppe „Current Serial Interface Configuration“ .....	118
Tabelle 152	WBM-Seite „Configuration of Serial Interface“ – Gruppe „Assign Mode of Serial Interface“ .....	118
Tabelle 153	WBM-Seite „Configuration of Serial Interface“ – Gruppe „Assign Owner of Serial Interface“ .....	118
Tabelle 154	WBM-Seite „Configuration of Serial Interface“ – Gruppe „Current Serial Interface Configuration“ .....	119
Tabelle 155	WBM-Seite „Configuration of Serial Interface“ – Gruppe „Bus Termination“ .....	119
Tabelle 156	WBM-Seite „Configuration of Serial Interface“ – Gruppe „Bias Network“ .....	119
Tabelle 157	WBM-Seite „Configuration of Service Interface“ – Gruppe „Assign Owner of Service Interface“ .....	119
Tabelle 158	WBM-Seite „Create bootable Image“ – Gruppe „Create bootable image from boot device“ .....	120
Tabelle 159	WBM-Seite „Firmware Backup“ – Gruppe „Firmware Backup“ .....	120
Tabelle 160	WBM-Seite „Firmware Restore“ – Gruppe „Firmware Restore“ .....	122
Tabelle 161	WBM-Seite „Active System“ – Gruppe „Boot Device“ .....	124
Tabelle 162	WBM-Seite „Active System“ – Gruppe „System n (Internal Flash)“ .....	124
Tabelle 163	WBM-Seite „Mass Storage“ – Gruppe „Devices“ .....	124
Tabelle 164	WBM-Seite „Mass Storage“ – Gruppe „Create new Filesystem on Memory Card“ .....	125
Tabelle 165	WBM-Seite „Software Uploads“ – Gruppe „Upload new Software“ .....	125
Tabelle 166	WBM-Seite „Configuration of Network Services“ – Gruppe „FTP“ .....	125
Tabelle 167	WBM-Seite „Configuration of Network Services“ – Gruppe „FTPES (explicit FTPS)“ .....	126
Tabelle 168	WBM-Seite „Configuration of Network Services“ – Gruppe „HTTP“ .....	126
Tabelle 169	WBM-Seite „Configuration of Network Services“ – Gruppe „HTTPS“ .....	126
Tabelle 170	WBM-Seite „Configuration of Network Services“ – Gruppe „I/O-CHECK“ .....	126
Tabelle 171	WBM-Seite „Configuration of NTP Client“ – Gruppe „NTP Client Configuration“ .....	127
Tabelle 172	WBM-Seite „PLC Runtime Services“ – Gruppe „CODESYS V3“ .....	127

Tabelle 173	WBM-Seite „SSH Server Settings“ – Gruppe „SSH Server“ .....	128
Tabelle 174	WBM-Seite „DHCP Server Configuration“ – Gruppe „DHCP Server Configuration Bridge <n>“ .....	128
Tabelle 175	WBM-Seite „Configuration of DNS Server“ – Gruppe „DNS Server“ .....	129
Tabelle 176	WBM-Seite „Overview“ – Gruppe „Connection <n>“ .....	130
Tabelle 177	WBM-Seite „Configuration of Connection <n>“ – Gruppe „Configuration“ .....	130
Tabelle 178	Anzeige der Auswahl- und Eingabefelder abhängig von der ausgewählten Cloud-Plattform.	132
Tabelle 179	Auswahlmöglichkeit des Datenprotokolls abhängig von der ausgewählten Cloud-Plattform	133
Tabelle 180	Anzeige der Auswahl- und Eingabefelder abhängig vom ausgewählten Datenprotokoll.....	133
Tabelle 181	Auswahlmöglichkeit des Cache-Modes abhängig vom ausgewählten Datenprotokoll .....	133
Tabelle 182	Anzeige der Eingabefelder abhängig von der ausgewählten Authentifizierung .....	133
Tabelle 183	WBM-Seite „Controls Settings“ – Gruppe „OMS Controls“ .....	134
Tabelle 184	WBM-Seite „Configuration of general SNMP parameters“ – Gruppe „General SNMP Configuration“ .....	134
Tabelle 185	WBM-Seite „Configuration of SNMP v1/v2c Parameters“ – Gruppe „Communities“ .....	135
Tabelle 186	WBM-Seite „Configuration of SNMP v1/v2cparameters“ – Gruppe „Trap Receivers“ .....	135
Tabelle 187	WBM-Seite „Configuration of SNMP v3 Parameters“ – Gruppe „Users“ .....	135
Tabelle 188	WBM-Seite „Configuration of SNMP v3 Parameters“ – Gruppe „Trap Receivers“ .....	136
Tabelle 189	WBM-Seite „Commissioning Settings“ – Gruppe „Commissioning“ .....	136
Tabelle 190	WBM-Seite „Docker Settings“ – Gruppe „Docker Status“ .....	137
Tabelle 191	WBM-Seite „WBM User Configuration“ – Gruppe „Change Passwords“ .....	138
Tabelle 192	WBM-Seite „OPC UA Configuration“ – Gruppe „OPC UA Server Configuration“ .....	138
Tabelle 193	WBM-Seite „OPC UA Configuration“ – Gruppe „OPC UA Server Security Settings“ .....	139
Tabelle 194	WBM-Seite „BACnet Status“ – Gruppe „BACnet Information“ .....	139
Tabelle 195	WBM-Seite „BACnet Status“ – Gruppe „BACnet License“ .....	140
Tabelle 196	WBM-Seite „BACnet Status“ – Gruppe „BACnet Data Link“ .....	140
Tabelle 197	WBM-Seite „BACnet Data Link“ – Gruppe „BACnet Restart“ .....	140
Tabelle 198	WBM-Seite „BACnet Configuration“ – Gruppe „BACnet Service“ .....	140
Tabelle 199	WBM-Seite „BACnet Configuration“ – Gruppe „BACnet Data“ .....	141
Tabelle 200	WBM-Seite „BACnet Configuration“ – Gruppe „BACnet Log Level“ .....	141
Tabelle 201	WBM-Seite „BACnet Configuration“ – Gruppe „BACnet Network Capture“ .....	141
Tabelle 202	WBM-Seite „BACnet Data Link“ – Gruppe „BACnet Restart“ .....	142
Tabelle 203	WBM-Seite „BACnet Data Link“ – Gruppe „BACnet/IP“ .....	142
Tabelle 204	WBM-Seite „BACnet Data Link“ – Gruppe „BACnet/SC“ .....	142
Tabelle 205	WBM-Seite „BACnet Data Link“ – Gruppe „BACnet/SC Certificate Authority (CA)“ .....	143
Tabelle 206	WBM-Seite „BACnet Data Link“ – Gruppe „BACnet/SC Certificate“ .....	143
Tabelle 207	WBM-Seite „BACnet Configuration“ – Gruppe „BACnet/SC Certificate Signing Request (CSR)“ .....	143
Tabelle 208	WBM-Seite „BACnet Data Link“ – Gruppe „BACnet/SC Default Certificates“ .....	143

Tabelle 209	WBM-Seite „BACnet Storage Location“ – Gruppe „BACnet Persistence“ .....	143
Tabelle 210	WBM-Seite „BACnet Storage Location“ – Gruppe „BACnet Trendlog“ .....	144
Tabelle 211	WBM-Seite „BACnet Storage Location“ – Gruppe „BACnet Eventlog“ .....	144
Tabelle 212	WBM-Seite „BACnet Info“ – Gruppe „Refresh Options“ .....	144
Tabelle 213	WBM-Seite „BACnet Info“ – Gruppe „BACnet/IP Statistics“ .....	145
Tabelle 214	WBM-Seite „BACnet Info“ – Gruppe „BACnet/SC Statistics“ .....	145
Tabelle 215	WBM-Seite „BACnet Info“ – Gruppe „BACnet/SC Connections“ .....	145
Tabelle 216	WBM-Seite „OpenVPN / IPsec“ – Gruppe „OpenVPN“ .....	146
Tabelle 217	WBM-Seite „OpenVPN / IPsec“ – Gruppe „IPsec“ .....	146
Tabelle 218	WBM-Seite „General Firewall Configuration“ – Gruppe „Global Firewall Parameter“ .....	146
Tabelle 219	WBM-Seite „Interface Configuration“ – Gruppe „Firewall Configuration Bridge <n> / VPN / WAN“ .....	147
Tabelle 220	Ports für Telecontrol-Funktionalität.....	148
Tabelle 221	WBM-Seite „Configuration of MAC address filter“ – Gruppe „Global MAC address filter state“ .....	148
Tabelle 222	WBM-Seite „Configuration of MAC address filter“ – Gruppe „MAC address filter state Bridge <n>“ .....	149
Tabelle 223	WBM-Seite „Configuration of MAC address filter“ – Gruppe „MAC address filter whitelist“ ...	149
Tabelle 224	WBM-Seite „Configuration of User Filter“ – Gruppe „User filter“ .....	149
Tabelle 225	WBM-Seite „Certificates“ – Gruppe „Installed Certificates“ .....	150
Tabelle 226	WBM-Seite „Certificates“ – Gruppe „Installed Private Keys“ .....	150
Tabelle 227	WBM-Seite „Boot mode configuration“ – Gruppe „Force internal boot“ .....	151
Tabelle 228	WBM-Seite „Security Settings“ – Gruppe „TLS Configuration“ .....	151
Tabelle 229	WBM-Seite „Advanced Intrusion Detection Environment (AIDE)“ – Gruppe „Run AIDE check at startup“ .....	151
Tabelle 230	WBM-Seite „Advanced Intrusion Detection Environment (AIDE)“ – Gruppe „Control AIDE and show log“ .....	152
Tabelle 231	WBM-Seite „WAGO Device Access“ – Gruppe „Unauthenticated Requests“ .....	153
Tabelle 232	WBM-Seite „WAGO Device Access“ – Gruppe „CORS Configuration“ .....	153
Tabelle 233	WBM-Seite „Log Message Viewer“ – Gruppe „Refresh Options“ .....	153
Tabelle 234	WBM-Seite „Download“ – Gruppe „Diagnostic Information“ .....	154
Tabelle 235	WBM-Seite „Network Capture“ – Gruppe „State“ .....	154
Tabelle 236	WBM-Seite „Network Capture“ – Gruppe „Configuration“ .....	154
Tabelle 237	WBM-Seite „Network Capture“ – Gruppe „Filter Configuration“ .....	155
Tabelle 238	WBM-Seite „Network Capture“ – Gruppe „Log Download“ .....	155

# Abbildungsverzeichnis

Abbildung 1	Kommunikationsschnittstelle, Busabschluss und Bias-Netzwerk.....	22
Abbildung 2	WBM-Browserfenster (Beispiel) .....	24
Abbildung 3	WBM-Kopfzeile mit nicht darstellbaren Registerkarten (Beispiel) .....	24
Abbildung 4	WBM-Statuszeile (Beispiel) .....	24
Abbildung 5	Anbindung der Controller an einen Cloud-Dienst (Beispiel).....	49
Abbildung 6	WAGO Ethernet Settings – Startbildschirm (Beispielbild) .....	84
Abbildung 7	WAGO Ethernet Settings – Register Netzwerk (Beispielbild) .....	84
Abbildung 8	Beispiel eines Funktionstests .....	87
Abbildung 9	Anmeldefenster .....	89
Abbildung 10	WBM-Browserfenster (Beispiel) .....	90
Abbildung 11	WBM-Kopfzeile mit nicht darstellbaren Registerkarten (Beispiel) .....	90
Abbildung 12	WBM-Statuszeile (Beispiel) .....	91
Abbildung 13	„WAGO Ethernet Settings“ – Startbildschirm (Beispiel) .....	93
Abbildung 14	„WAGO Ethernet Settings“ – Kommunikationsverbindung (Beispiel).....	94
Abbildung 15	„WAGO Ethernet Settings“ – Registerkarte Identifikation (Beispiel) .....	95
Abbildung 16	„WAGO Ethernet Settings“ – Registerkarte Netzwerk (Beispiel) .....	95
Abbildung 17	„WAGO Ethernet Settings“ – Registerkarte Protokoll (Beispiel).....	96
Abbildung 18	„WAGO Ethernet Settings“ – Registerkarte Status (Beispiel) .....	97

**WAGO GmbH & Co. KG**

Postfach 2880 · D - 32385 Minden  
Hansastraße 27 · D - 32423 Minden

✉ [info@wago.com](mailto:info@wago.com)

🌐 [www.wago.com](http://www.wago.com)

Zentrale

+49 (0) 571/887 – 0

Vertrieb

+49 (0) 571/887 – 44 222

Auftragservice

+49 (0) 571/887 – 44 333

WAGO ist eine eingetragene Marke der WAGO Verwaltungsgesellschaft mbH.

Copyright – WAGO GmbH & Co. KG – Alle Rechte vorbehalten. Inhalt und Struktur der WAGO Websites, Kataloge, Videos und andere WAGO Medien unterliegen dem Urheberrecht. Die Verbreitung oder Veränderung des Inhalts dieser Seiten und Videos ist nicht gestattet. Des Weiteren darf der Inhalt weder zu kommerziellen Zwecken kopiert, noch Dritten zugänglich gemacht werden. Dem Urheberrecht unterliegen auch die Bilder und Videos, die der WAGO GmbH & Co. KG von Dritten zur Verfügung gestellt wurden.