WAGO TECHDOCS

Handbuch

WAGO Edge Controller

752-8303/8000-0002

Version 1.5.0, gültig ab FW-Version 04.05.08(27)

© 2024 WAGO GmbH & Co. KG
Alle Rechte vorbehalten.

WAGO GmbH & Co. KG

Hansastraße 27
D-32423 Minden

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

E-Mail: info@wago.com

Web: www.wago.com

Technischer Support

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

E-Mail: support@wago.com

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

E-Mail: documentation@wago.com

Wir weisen darauf hin, dass die im Handbuch 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

1 Bestimmungen 8
1.1 Gültigkeitsbereich 8
1.2 Dokumentportfolio 8
1.3 Urheberschutz 8
1.4 Schutzrechte 9
1.5 Symbole 11
1.6 Darstellung der Zahlensysteme 12
1.7 Schriftkonventionen 12
1.8 Rechtliche Grundlagen 13
1.8.1 Änderungsvorbehalt 13
1.8.2 Personalqualifikation 13
1.8.3 Bestimmungsgemäße Verwendung 13
1.8.3.1 Sachwidrige Verwendung 13
1.8.3.2 Gewährleistung und Haftung 14
1.8.3.3 Pflichten von Errichter/Betreiber 14

2 Sicherheit 15
2.1 Sicherheitshinweise 15
2.2 Spezielle Einsatzbestimmungen 17

3 Überblick 18

4 Eigenschaften 19
4.1 Ansicht 19
4.2 Bedruckung 20
4.3 Anschlüsse 22
4.3.1 Anschlüsse auf der Vorderseite 22
4.3.2 Anschlüsse oben 22
4.3.3 „X1“ und „X2“ – ETHERNET-Schnittstellen 23
4.3.4 „X3“ – Serielle Schnittstelle RS-232/-485 23
4.3.4.1 Betrieb als RS-232-Schnittstelle 24
4.3.4.2 Betrieb als RS-485-Schnittstelle 25
4.3.5 „X4“ – CAN-Schnittstelle 25
4.3.6 „X5“ – Versorgungsanschluss POWER 26
4.3.7 „X6“ und „X7“ – USB-2.0-Schnittstellen 26
4.3.8 „X8“ – Lineout-Audioausgang (Kopfhörer) 26
4.3.9 „X9“ – HDMI-Schnittstelle Typ A 27
4.3.10 „X10“ – USB-C-Schnittstelle 27
4.3.11 „X11“ – 4 Digitale Ein- und Ausgänge DIO 27
4.3.12 „µSD“ – Speicherkartensteckplatz 28
4.4 Echtzeituhr 30
4.5 Anzeigeelemente 31
4.5.1 Status-LED 31
4.6 Bedienelemente 32
4.6.1 Betriebsartenschalter 32
4.6.2 Taster „CFG/RST“ 32
4.7 Schematisches Schaltbild 33
4.8 Technische Daten 34

4.8.1 Gerät ... 34
4.8.2 Klimatische Umgebungsbedingungen ... 34
4.8.3 Spannungsversorgung ... 34
4.8.4 Hardware ... 35
4.8.5 Kommunikation ... 35
4.8.6 Schnittstellen ... 35
4.8.7 Anschlüsse ... 36
4.9 Zulassungen ... 37
4.10 Normen und Richtlinien ... 37

5 Funktionen ... 38

5.1 Webbrowser ... 38
5.2 Verbindungsüberwachung ... 39
5.3 WBM für Konfigurieren/Parametrieren ... 39
5.4 Netzwerk ... 39
5.4.1 Schnittstellenkonfiguration ... 39
5.4.1.1 Betrieb mit getrennten Netzwerk-Schnittstellen ... 39
5.4.2 Netzwerksicherheit ... 39
5.4.2.1 Benutzer (User) und Passwörter ... 39
5.4.2.2 Dienste und Benutzer ... 40
5.4.2.3 WBM-Benutzergruppe ... 40
5.4.2.4 Linux®-Benutzergruppe ... 41
5.4.2.5 SNMP-Benutzergruppe ... 42
5.4.2.6 Webserverauthentifizierung ... 42
5.4.2.7 TLS-Verschlüsselung ... 42
5.4.3 Netzwerkkonfiguration ... 43
5.4.3.1 Hostname/Domainname ... 43
5.4.3.2 Default-Gateways ... 43
5.5 Speicherkartenfunktionen ... 44
5.5.1 Backup ... 44
5.5.2 Restore ... 44
5.5.3 Create Image ... 45
5.6 Nachladen von Software ... 45
5.7 Booten ... 46
5.8 Lizenzpflichtige Softwarekomponenten ... 48

6 Montieren ... 49

6.1 Aufbaurichtlinien und Normen ... 49
6.2 Einbaulagen ... 49
6.3 Montage auf Tragschiene ... 50

7 Anschließen ... 51

7.1 Erden ... 51
7.2 Geräte anschließen ... 51
7.3 Versorgungsspannung anschließen ... 52

8 In Betrieb nehmen ... 53

8.1 Einschalten ... 53
8.2 Log-in ... 53
8.3 Ermitteln der IP-Adresse des Host-PC ... 53
8.4 Einstellen einer IP-Adresse ... 54

8.4.1 IP-Verbindung über USB ... 54
8.4.2 Ändern einer IP-Adresse mit „WAGO Ethernet Settings“ ... 55
8.4.3 Temporär eine feste IP-Adresse einstellen ... 56
8.4.4 Einstellen der IP-Adresse über das WBM ... 57
8.4.5 Zuweisen einer IP-Adresse mittels DHCP ... 58
8.5 Reset-Funktionen auslösen ... 58
8.5.1 Warmstart-Reset ... 58
8.5.2 Kaltstart-Reset ... 59
8.5.3 Software-Reset (Neustart) ... 59
8.5.4 Factory-Reset ... 59
8.6 Im Web-Based-Management (WBM) konfigurieren ... 61
8.6.1 Benutzerverwaltung des WBM ... 63
8.6.2 Allgemeine Seiteninformationen ... 68
8.6.3 Reboot-Funktion ... 70

9 Laufzeitumgebung CODESYS V3 ... 71

9.1 Grundlegende Hinweise ... 71
9.2 CODESYS V3-Prioritäten ... 72
9.3 Speicherbereiche unter CODESYS V3 ... 73
9.3.1 Programm- und Datenspeicher ... 73
9.3.2 Bausteinbegrenzung ... 73
9.3.3 Remanenter Arbeitsspeicher ... 73
9.3.4 Dateizugriff aus der IEC-Applikation ... 73
9.3.5 Netzwerkeinstellungen durch die IEC-Applikation ändern ... 74
9.3.6 EtherCAT ... 74

10 Diagnose ... 75

11 Service ... 76

11.1 Konfiguration mit dem WBM ändern ... 76
11.2 Firmwareänderungen ... 77
11.2.1 Firmware-Update/-Downgrade mit WAGOupload durchführen ... 78
11.2.2 Firmware-Update/-Downgrade mit Speicherkarte und WBM durchführen ... 79

12 Demontieren ... 80

12.1 Demontage von der Tragschiene ... 80

13 Entsorgen ... 81

13.1 Elektro- und Elektronikgeräte ... 81
13.2 Verpackung ... 81

14 Zubehör ... 83

15 Anhang ... 84

15.1 Konfigurationsdialoge ... 84
15.1.1 Web-Based-Management (WBM) ... 84
15.1.1.1 Registerkarte „Information“ ... 84
15.1.1.1.1 Seite „Device Status“ ... 84
15.1.1.1.2 Seite „Vendor Information“ ... 86
15.1.1.1.3 Seite „PLC Runtime Information“ ... 87
15.1.1.1.4 Seite „WAGO Software License Agreement“ ... 88
15.1.1.1.5 Seite „Open Source Licenses“ ... 89

15.1.1.1.6 Seite „WBM Third Party License Information“ 90
15.1.1.1.7 Seite „Trademarks Information“ 91
15.1.1.1.8 Seite „WBM Version“ 92
15.1.1.2 Registerkarte „Configuration“ 93
15.1.1.2.1 Seite „PLC Runtime Configuration“ 93
15.1.1.2.2 Seite „TCP/IP Configuration“ 95
15.1.1.2.3 Seite „Ethernet Configuration“ 97
15.1.1.2.4 Seite „Configuration of Host and Domain Name“ 101
15.1.1.2.5 Seite „Routing“ 103
15.1.1.2.6 Seite „Spanning Tree Protocol“ 108
15.1.1.2.7 Seite „Clock Settings“ 112
15.1.1.2.8 Seite „Configuration of Serial Interface“ 114
15.1.1.2.9 Seite „Configuration of Service Interface“ 116
15.1.1.2.10 Seite „Create bootable Image“ 117
15.1.1.2.11 Seite „Firmware Backup“ 118
15.1.1.2.12 Seite „Firmware Restore“ 120
15.1.1.2.13 Seite „Active System“ 122
15.1.1.2.14 Seite „Mass Storage“ 123
15.1.1.2.15 Seite „Software Uploads“ 124
15.1.1.2.16 Seite „Configuration of Network Services“ 125
15.1.1.2.17 Seite „Configuration of NTP Client“ 127
15.1.1.2.18 Seite „PLC Runtime Services“ 128
15.1.1.2.19 Seite „SSH Server Settings“ 129
15.1.1.2.20 Seite „DHCP Server Configuration“ 130
15.1.1.2.21 Seite „Configuration of DNS Server“ 131
15.1.1.2.22 Seite „Status overview“ 132
15.1.1.2.23 Seite „Configuration of Connection <n>“ 133
15.1.1.2.24 Seite „Configuration of General SNMP Parameters“ 140
15.1.1.2.25 Seite „Configuration of SNMP v1/v2c Parameters“ 141
15.1.1.2.26 Seite „Configuration of SNMP v3 Parameters“ 143
15.1.1.2.27 Seite „Favorites“ 147
15.1.1.2.28 Seite „Autostart“ 149
15.1.1.2.29 Seite „Monitoring“ 150
15.1.1.2.30 Seite „Browser Security“ 151
15.1.1.2.31 Seite „Commissioning Settings“ 152
15.1.1.2.32 Seite „Docker Settings“ 153
15.1.1.2.33 Seite „Fonts“ 154
15.1.1.2.34 Seite „Display Orientation“ 155
15.1.1.2.35 Seite „Screensaver“ 156
15.1.1.2.36 Seite „WBM User Configuration“ 158
15.1.1.3 Registerkarte „Fieldbus“ 159
15.1.1.3.1 Seite „OPC UA Configuration“ 159
15.1.1.3.1 Seite „BACnet Status“ 161
15.1.1.3.2 Seite „BACnet Configuration“ 162
15.1.1.3.3 Seite „BACnet Data Link“ 165
15.1.1.3.4 Seite „BACnet Storage Location“ 169
15.1.1.4 Registerkarte „Security“ 171
15.1.1.4.1 Seite „OpenVPN / IPsec Configuration“ 171
15.1.1.4.2 Seite „General Firewall Configuration“ 173
15.1.1.4.3 Seite „Interface Configuration“ 174

15.1.1.4.4 Seite „Configuration of MAC address filter“ 176
15.1.1.4.5 Seite „Configuration of User Filter“ 179
15.1.1.4.6 Seite „Certificates“ 181
15.1.1.4.7 Seite „Boot mode configuration“ 182
15.1.1.4.8 Seite „Security Settings“ 183
15.1.1.4.9 Seite „Advanced Intrusion Detection Environment (AIDE)“ 184
15.1.1.4.10 Seite „WAGO Device Access“ 186
15.1.1.5 Registerkarte „Diagnostic“ 187
15.1.1.5.1 Seite „Log Message Viewer“ 187
15.1.1.5.2 Seite „Download“ 188
15.1.1.5.3 Seite „Network Capture“ 189

Abbildungsverzeichnis 193

Tabellenverzeichnis 194

1 Bestimmungen

Das WAGO Produkt darf nur nach den Anweisungen dieser Dokumentation installiert und betrieben werden.

Hinweis

Dokumentation aufbewahren!
Diese Dokumentation ist Teil des Produkts. Bewahren Sie deshalb die Dokumentation während der gesamten Nutzungsdauer des Produkts auf. Geben Sie die Dokumentation an jeden nachfolgenden Benutzer des Produkts weiter. Stellen Sie darüber hinaus sicher, dass gegebenenfalls jede erhaltene Ergänzung in die Dokumentation mit aufgenommen wird.

1.1 Gültigkeitsbereich

Die vorliegende Dokumentation gilt für das Produkt 752-8303/8000-0002.

1.2 Dokumentportfolio

Außer diesem Handbuch sollten Sie noch weitere WAGO Unterlagen benutzen:

- WAGO I/O SYSTEM 750, Handbuch zum eingesetzten Controller PFC
- WAGO I/O SYSTEM 750, Handbuch „Cyber-Security für Controller PFC100/PFC200“
- Migrationsleitfaden; Migration von ***e!****COCKPIT* zu CODESYS V3.5
- Technologiehandbuch „Industrial ETHERNET“

Diese Unterlagen stehen auf der WAGO Website www.wago.com zum Download zur Verfügung.

Weitere Informationen zu CODESYS V3.5 finden Sie in der CODESYS Onlinehilfe unter help.codesys.com (bis Servicepack 17) und in der neuen Onlinehilfe unter de.helpme-codesys.com (aktuelles Servicepack).

1.3 Urheberschutz

Diese Dokumentation, einschließlich aller darin befindlichen Abbildungen, ist urheberrechtlich geschützt. Jede Weiterverwendung dieser Dokumentation, die von den urheberrechtlichen Bestimmungen abweicht, ist nicht gestattet. Die Reproduktion, Übersetzung in andere Sprachen sowie die elektronische und fototechnische Archivierung und Veränderung bedarf der schriftlichen Genehmigung der WAGO GmbH & Co. KG, Minden. Zuwiderhandlungen ziehen einen Schadenersatzanspruch nach sich.

1.4 Schutzrechte

In dieser Dokumentation werden Marken Dritter verwendet. Die verwendeten Marken entnehmen Sie diesem Kapitel. Im Weiteren wird auf das Mitführen der Zeichen „®“ und „™“ verzichtet.

- Adobe® und Acrobat® sind eingetragene Marken der Adobe Systems Inc.
- Android™ ist eine Marke von Google LLC.
- Apple, das Apple-Logo, iPhone, iPad und iPod touch sind eingetragene Marken von Apple Inc., registriert in den U.S.A. und anderen Staaten. „App Store“ ist eine Dienstleistungsmarke von Apple Inc.
- AS-Interface® ist eine eingetragene Marke der AS-International Association e.V.
- BACnet® ist eine eingetragene Marke der American Society of Heating, Refrigerating and Air Conditioning Engineers, Inc. (ASHRAE).
- *Bluetooth*® ist ein registriertes Warenzeichen der Bluetooth SIG, Inc.
- CiA® und CANopen® sind eingetragene Marken des CAN in AUTOMATION – International Users and Manufacturers Group e. V.
- CODESYS ist eine eingetragene Marke der CODESYS Development GmbH.
- DALI ist eine eingetragene Marke der Digital Illumination Interface Alliance (DiiA).
- EtherCAT® ist eine eingetragene Marke und patentierte Technologie, lizenziert durch die Beckhoff Automation GmbH, Deutschland.
- EtherNet/IP™ ist eine eingetragene Marke der Open DeviceNet Vendor Association, Inc (ODVA).
- EnOcean® ist eine eingetragene Marke der EnOcean GmbH.
- Google Play™ ist ein eingetragenes Markenzeichen von Google Inc.
- IO-Link ist eine eingetragene Marke der PROFIBUS Nutzerorganisation e.V.
- KNX® ist eine eingetragene Marke der KNX Association cvba.
- Linux® ist eine eingetragene Marke von Linus Torvalds.
- LON® ist eine eingetragene Marke der Echelon Corporation.
- Modbus® ist eine registrierte Marke der Schneider Electric, lizenziert für die Modbus Organization, Inc.

- OPC UA ist eine registrierte Marke der OPC Foundation.
- PROFIBUS® ist eine registrierte Marke der PROFIBUS Nutzerorganisation e.V. (PNO).
- PROFINET® ist eine registrierte Marke der PROFIBUS Nutzerorganisation e.V. (PNO).
- QR Code ist eine registrierte Marke von DENSO WAVE INCORPORATED.
- Subversion® ist eine Marke der Apache Software Foundation.
- Windows® ist eine registrierte Marke der Microsoft Corporation.

1.5 Symbole

GEFAHR

Warnung vor Personenschäden!
Kennzeichnet eine unmittelbare Gefährdung mit hohem Risiko, die Tod oder schwere Körperverletzung zur Folge haben wird, wenn sie nicht vermieden wird.

GEFAHR

Warnung vor Personenschäden durch elektrischen Strom!
Kennzeichnet eine unmittelbare Gefährdung mit hohem Risiko, die Tod oder schwere Körperverletzung zur Folge haben wird, wenn sie nicht vermieden wird.

WARNUNG

Warnung vor Personenschäden!
Kennzeichnet eine mögliche Gefährdung mit mittlerem Risiko, die Tod oder (schwere) Körperverletzung zur Folge haben kann, wenn sie nicht vermieden wird.

VORSICHT

Warnung vor Personenschäden!
Kennzeichnet eine mögliche Gefährdung mit geringem Risiko, die leichte oder mittlere Körperverletzung zur Folge haben könnte, wenn sie nicht vermieden wird.

ACHTUNG

Warnung vor Sachschäden!
Kennzeichnet eine mögliche Gefährdung, die Sachschaden zur Folge haben könnte, wenn sie nicht vermieden wird.

ESD

Warnung vor Sachschäden durch elektrostatische Aufladung!
Kennzeichnet eine mögliche Gefährdung, die Sachschaden zur Folge haben könnte, wenn sie nicht vermieden wird.

Hinweis

Wichtiger Hinweis!
Kennzeichnet eine mögliche Fehlfunktion, die aber keinen Sachschaden zur Folge hat, wenn sie nicht vermieden wird.

Information

Weitere Information
Weist auf weitere Informationen hin, die kein wesentlicher Bestandteil dieser Dokumentation sind (z. B. Internet).

1.6 Darstellung der Zahlensysteme

Tabelle 1: Darstellungen der Zahlensysteme

Zahlensystem	Beispiel	Bemerkung
Dezimal	100	Normale Schreibweise
Hexadezimal	0x64	C-Notation
Binär	'100' '0110.0100'	In Hochkomma, Nibble durch Punkt getrennt

1.7 Schriftkonventionen

Tabelle 2: Schriftkonventionen

Schriftart	Bedeutung
kursiv	Namen von Pfaden und Dateien werden kursiv dargestellt z. B.: *C:\Programme\WAGO Software*
Menü	Menüpunkte werden fett dargestellt z. B.: **Speichern**
>	Ein „Größer als“- Zeichen zwischen zwei Namen bedeutet die Auswahl eines Menüpunktes aus einem Menü z. B.: **Datei > Neu**
Eingabe	Bezeichnungen von Eingabe- oder Auswahlfeldern werden fett dargestellt z. B.: **Messbereichsanfang**
„Wert“	Eingabe- oder Auswahlwerte werden in Anführungszeichen dargestellt z. B.: Geben Sie unter **Messbereichsanfang** den Wert „4 mA“ ein.
[Button]	Schaltflächenbeschriftungen in Dialogen werden fett dargestellt und in eckige Klammern eingefasst z. B.: **[Eingabe]**
[Taste]	Tastenbeschriftungen auf der Tastatur werden fett dargestellt und in eckige Klammern eingefasst z. B.: **[F5]**

1.8 Rechtliche Grundlagen

1.8.1 Änderungsvorbehalt

Die WAGO GmbH & Co. KG behält sich Änderungen vor. Alle Rechte für den Fall der Patenterteilung oder des Gebrauchsmusterschutzes sind der WAGO GmbH & Co. KG vorbehalten. Fremdprodukte werden stets ohne Vermerk auf Patentrechte genannt. Die Existenz solcher Rechte ist daher nicht auszuschließen.

1.8.2 Personalqualifikation

Sämtliche Arbeitsschritte, die an den Geräten der Serie 752 durchgeführt werden, dürfen nur von Elektrofachkräften mit ausreichenden Kenntnissen im Bereich der Automatisierungstechnik vorgenommen werden. Diese müssen mit den aktuellen Normen und Richtlinien für die Geräte und das Automatisierungsumfeld vertraut sein.

Alle Eingriffe in die Steuerung sind stets von Fachkräften mit ausreichenden Kenntnissen in der SPS-Programmierung durchzuführen.

1.8.3 Bestimmungsgemäße Verwendung

Der Edge Controller ist für den Einsatz im Bereich der Regelungs-, Steuerungs- und Automationstechnik geeignet. Der Einsatz erstreckt sich über den Bereich in Wohn- und Gewerbegebieten sowie im Industriebereich. In allen Anwendungsfällen ist darauf zu achten, dass die technischen Daten eingehalten werden.

Im Wohn-, Geschäfts- und Gewerbebereich sowie in Kleinbetrieben ist die Verwendung der HDMI-Schnittstelle nicht zulässig.
Im Industriebereich ist die Verwendung der HDMI-Schnittstelle zulässig.

Das Produkt ist ein offenes Betriebsmittel und ist für den Einbau in ein zusätzliches Gehäuse konzipiert.
Das Produkt genügt der Schutzart IP20 und ist für den Einsatz in trockenen Innenräumen ausgelegt.

1.8.3.1 Sachwidrige Verwendung

Eine sachwidrige Verwendung des Produktes ist nicht gestattet. Die sachwidrige Verwendung ist insbesondere in den folgenden Fällen gegeben:

- Nichtbeachten der bestimmungsgemäßen Verwendung.
- Einsatz ohne Schutzmaßnahmen in einer Umgebung, in der Feuchtigkeit, Salzwasser, Salzsprühnebel, Staub, ätzende Dämpfe, Gase, direkte Sonneneinstrahlung oder ionisierende Strahlung auftreten können.

- Verwendung des Produktes in Bereichen mit besonderem Risiko, die einen fehlerfreien Dauerbetrieb erfordern und in denen ein Ausfall oder Betrieb des Produktes zu einer unmittelbaren Gefahr für Leben, Körper oder Gesundheit oder zu erheblichen Sach- oder Umweltschäden führen kann (wie der Betrieb von Kernkraftwerken, Waffensystemen, Luft- und Kraftfahrzeugen).

1.8.3.2 Gewährleistung und Haftung

Es gelten die Bestimmungen der Allgemeinen Geschäfts- und Vertragsbedingungen für Lieferungen und Leistungen der WAGO GmbH & Co. KG sowie für Softwareprodukte und Produkte mit integrierter Software der WAGO Software-Lizenzvertrag, beide abrufbar unter: www.wago.com. Danach ist die Gewährleistung insbesondere in folgenden Fällen ausgeschlossen:

- Das Produkt wird sachwidrig verwendet.
- Der Mangel beruht auf speziellen Vorgaben (Hard- und Softwarekonfigurationen).
- Es wurden Modifikationen der Hard- oder Software durch den Nutzer oder Dritte durchgeführt, die nicht in dieser Dokumentation beschrieben sind und für das Auftreten des Mangels zumindest mitursächlich sind.

Einzelvertragliche Abreden haben stets Vorrang.

1.8.3.3 Pflichten von Errichter/Betreiber

Die Verantwortung für die Sicherheit einer mit dem Produkt errichteten Anlage bzw. eines Systems liegt beim Errichter/Betreiber. Der Errichter/Betreiber ist für den sachgemäßen Einbau und die Sicherheit in den Anlagen verantwortlich. Dieser muss die geltenden Gesetze, Normen, Bestimmungen, örtlichen Vorschriften, den Stand und die Regeln der Technik zum Zeitpunkt der Installation einhalten und die in der Gebrauchsanleitung beschriebenen Vorgaben beachten. Ferner müssen die Errichtungsbestimmungen der Zulassungen eingehalten werden. Bei Nichteinhaltung darf das Produkt nicht im Geltungsbereich der Zulassung betrieben werden.

2 Sicherheit

2.1 Sicherheitshinweise

Dieses Kapitel beinhaltet ausschließlich eine Zusammenfassung der wichtigsten Sicherheitsbestimmungen und Hinweise. Diese werden in den einzelnen Kapiteln wieder aufgenommen. Zum Schutz vor Personenschäden und zur Vorbeugung von Sachschäden an Geräten ist es notwendig, die Sicherheitsrichtlinien sorgfältig zu lesen und einzuhalten.

Beim Einbauen des Gerätes in Ihre Anlage und während des Betriebes sind folgende Sicherheitshinweise zu beachten:

GEFAHR

Nicht an Geräten unter Spannung arbeiten!
Gefährliche elektrische Spannung kann zu elektrischem Schlag und Verbrennungen führen.
Schalten Sie immer denjenigen Anlagenteil spannungsfrei, an dem Sie das Gerät montieren bzw. demontieren wollen!

GEFAHR

Nur SELV-Spannungsquelle verwenden!
Betreiben Sie das Gerät ausschließlich mit einer SELV- (Safety Extra Low Voltage) Spannungsquelle, die die Anforderungen einer LPS (Limited Power Source) gemäß DIN EN 60950-1 erfüllt.

GEFAHR

Unfallverhütungsvorschriften beachten!
Beachten Sie bei Montage, Inbetriebnahme, Betrieb, Wartung und Störbehebung die für Ihre Maschine/Anlage zutreffenden Unfallverhütungsvorschriften wie beispielsweise die DGUV Vorschrift 3 „Elektrische Anlagen und Betriebsmittel“.

GEFAHR

Auf normgerechten Anschluss achten!
Zur Vermeidung von Gefahren für das Personal und Störungen an Ihrer Anlage, verlegen Sie die Daten- und Versorgungsleitungen normgerecht und achten Sie auf die korrekte Anschlussbelegung. Beachten Sie die für Ihre Anwendung zutreffenden EMV-Richtlinien.

ACHTUNG

IP-Schutzart beachten!
Das Gerät ist ein offenes Betriebsmittel, das IP20 entspricht. Wenn die Betriebsumgebung diese Anforderungen nicht erfüllt, müssen Sie das Gerät in einen Schaltschrank oder in ein Gehäuse einbauen.

ACHTUNG

Defekte oder beschädigte Geräte austauschen!
Tauschen Sie defekte oder beschädigte Geräte (z. B. bei deformierten Kontakten) aus.

ACHTUNG

Geräte vor kriechenden und isolierenden Stoffen schützen!
Die Geräte sind unbeständig gegen Stoffe, die kriechende und isolierende Eigenschaften besitzen, z. B. Aerosole, Silikone, Triglyceride (Bestandteil einiger Handcremes). Sollten Sie nicht ausschließen können, dass diese Stoffe im Umfeld der Geräte auftreten, bauen Sie die Geräte in ein Gehäuse ein, das resistent gegen oben genannte Stoffe ist. Verwenden Sie generell zur Handhabung der Geräte saubere Werkzeuge und Materialien.

ACHTUNG

Nur mit zulässigen Materialien reinigen!
Reinigen Sie das Gehäuse und verschmutzte Kontakte mit Propanol.

ACHTUNG

Kein Kontaktspray verwenden!
Verwenden Sie kein Kontaktspray, da in Verbindung mit Verunreinigungen die Funktion der Kontaktstelle beeinträchtigt werden kann.

ACHTUNG

Nicht in Telekommunikationsnetzen einsetzen!
Verwenden Sie Geräte mit ETHERNET-/RJ-45-Anschluss ausschließlich in LANs. Verbinden Sie diese Geräte niemals mit Telekommunikationsnetzen, wie z. B. mit Analog- oder ISDN-Telefonanlagen.

ESD

Elektrostatische Entladung vermeiden!
In den Geräten sind elektronische Komponenten integriert, die Sie durch elektrostatische Entladung bei Berührung zerstören können. Beachten Sie die Sicherheitsmaßnahmen gegen elektrostatische Entladung gemäß DIN EN 61340-5-1/-3. Achten Sie beim Umgang mit den Geräten auf gute Erdung der Umgebung (Personen, Arbeitsplatz und Verpackung).

2.2 Spezielle Einsatzbestimmungen

Wo nicht speziell beschrieben, sind ETHERNET-Geräte für den Einsatz in lokalen Netzwerken bestimmt. Beachten Sie folgende Hinweise, wenn Sie ETHERNET-Geräte in Ihrer Anlage einsetzen:

- Verbinden Sie Steuerungskomponenten und Steuerungsnetzwerke nicht mit einem offenen Netzwerk wie dem Internet oder einem Büronetzwerk. WAGO empfiehlt, Steuerungskomponenten und Steuerungsnetzwerke hinter einer Firewall anzubringen.
- Schließen Sie alle nicht von Ihrer Applikation benötigten Ports und Dienste in den Steuerungskomponenten (z. B. für CODESYS), um die Gefahr von Cyber-Angriffen zu verringern und damit die Cyber-Security zu erhöhen. Öffnen Sie die Ports und Dienste nur für die Dauer der Inbetriebnahme bzw. Konfiguration.
- Beschränken Sie den physikalischen und elektronischen Zugang zu sämtlichen Automatisierungskomponenten auf einen autorisierten Personenkreis.
- Ändern Sie vor der ersten Inbetriebnahme unbedingt die standardmäßig eingestellten Passwörter! Sie verringern so das Risiko, dass Unbefugte Zugriff auf Ihr System erhalten.
- Ändern Sie regelmäßig die verwendeten Passwörter! Sie verringern so das Risiko, dass Unbefugte Zugriff auf Ihr System erhalten.
- Führen Sie regelmäßig eine Bedrohungsanalyse durch. So können Sie prüfen, ob die getroffenen Maßnahmen Ihrem Schutzbedürfnis entsprechen.
- Wenden Sie in der sicherheitsgerichteten Gestaltung Ihrer Anlage „Defense-in-depth“-Mechanismen an, um den Zugriff und die Kontrolle auf individuelle Produkte und Netzwerke einzuschränken.

Hinweis

Beachten Sie die Risiken bei der Nutzung von Cloud-Diensten!
Wenn Sie fremde Cloud-Dienste nutzen, lagern Sie schützenswerte Daten in eigener Verantwortung an einen Cloud-Anbieter aus. Durch Zugriffe von außen können manipulierte Daten und/oder ungewollte Steuerungsbefehle die Funktionsfähigkeit Ihrer Steuerungsanlage beeinträchtigen.

Nutzen Sie Verschlüsselungsverfahren, um Ihre Daten zu schützen und beachten Sie hierbei die Hinweise des Bundesamts für Sicherheit in der Informationstechnik „Cloud: Risiken und Sicherheitstipps“.
Beachten Sie vergleichbare Publikationen der zuständigen Stellen Ihres Landes.

3 Überblick

Der Controller vereint HMI- und Steuerungsaufgaben und kann somit eine PLC-Steuerung ersetzen. Visu-Software und Runtime-Software laufen beide auf dem Controller. Er ist zur Montage auf einer Hutschiene geeignet und zeichnet sich durch verschiedene Schnittstellen aus.

Die Schnittstellen umfassen ETHERNET, USB, microSD, Lineout (Kopfhörerausgang) und HDMI.

Die Schnittstellen umfassen außerdem digitale Ein- und Ausgänge, eine RS-232/RS-485- und eine CAN-Schnittstelle zur Anbindung von zusätzlichen I/Os.

Der Controller hat außerdem ein NVRAM.

4 Eigenschaften

4.1 Ansicht

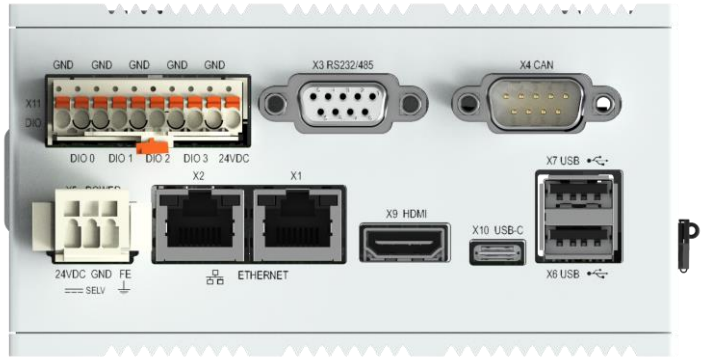

Abbildung 1: Ansicht Vorderseite

Auf der **Vorderseite** befinden sich die Anschlüsse. Details siehe Kapitel „Eigenschaften“ > „Anschlüsse“.

Abbildung 2: Ansicht oben

Oben befinden sich der Anschluss „X8 Lineout“, der Betriebsartenschalter (BAS) mit den Stellungen RESET-STOP-RUN, der Taster „CFG/RST“, die LEDs „SYS, RUN, CAN, H11, H22“ und der Speicherkarten-Steckplatz „µSD“. Details siehe Kapitel „Eigenschaften“ > „Anschlüsse“ > „Anzeigeelemente“ und > „Bedienelemente“.

4.2 Bedruckung

Die Bedruckung und das Typenschild befinden sich auf der Unterseite.
Folgende Angaben zum Produkt sind darin enthalten:

Tabelle 3: Bedruckung

Feld	Beispiel
Versorgungsspannung	24V SELV [−25 % … +30 %], LPS
Schutzklasse	Class III
IP-Schutzart	IP20

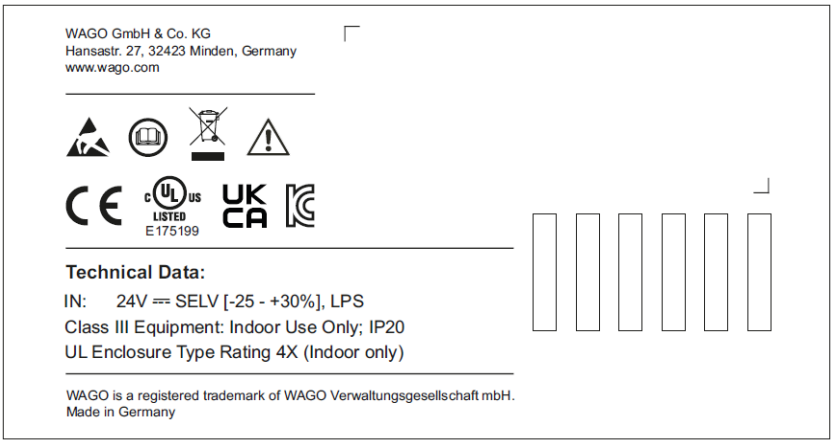

Abbildung 3: Bedruckung (Beispiel)

Tabelle 4: Typenschild

Feld	Beispiel
Bestellnummer	ITEM-NO.: 0752-8303/8000-0002
Artikelbezeichnung 1	Edge Controller
Artikelbezeichnung 2	EC PIO3
Kontrollnummer	24703.5303
Fertigungsdatum (Jahr – Monat)	2021-02
Freigabeindice: Hardwareversion	 01
Leistungsaufnahme	Pmax.=9,4 W
Versorgungsspannung	U=SELV 24V DC (−25 % … +30 %), LPS
Seriennummer	SN:37SUN31564010260448761+0 000000002331381
Barcode (Strichcode)	
DataMatrix-Code	

Abbildung 4: Typenschild (Beispiel)

4.3 Anschlüsse

4.3.1 Anschlüsse auf der Vorderseite

Tabelle 5: Anschlüsse auf der Vorderseite

Anschluss	Funktion
X1 und X2	ETHERNET-Schnittstellen mit LED-Anzeigen
X3	Serielle Schnittstelle RS-232 oder RS-485
X4	CAN-Schnittstelle
X5	POWER. Einspeisung der Versorgungsspannung
X6 und X7	USB-2.0-Host-Schnittstellen
X9	HDMI-Schnittstelle
X10	USB-C-Schnittstelle
X11	4 digitale Ein- und Ausgänge DIO

4.3.2 Anschlüsse oben

Tabelle 6: Anschlüsse oben

Anschluss	Funktion
X8	Lineout-Audioausgang (Kopfhörer)
µSD	Steckplatz für microSD- und microSDHC-Speicherkarten, mit Abdeckklappe, verplombbar

4.3.3 „X1“ und „X2“ – ETHERNET-Schnittstellen

Die ETHERNET-Schnittstellen sind als RJ-45-Buchsen ausgeführt. Die orangefarbene LED leuchtet bei LINK und die grüne LED blinkt bei Datentransfer.

Die Anschlüsse und Leitungen entsprechen Kategorie 5e und den Richtlinien für ETHERNET-Schnittstellen.

Der integrierte 10/100 Mbit-ETHERNET-Switch unterstützt Auto-MDI(X). Es können sowohl Crossover- als auch Patch-Kabel verwendet werden.

4.3.4 „X3“ – Serielle Schnittstelle RS-232/-485

Diese Schnittstelle ist als D-Sub-9-Einbaubuchse ausgeführt und ist galvanisch von der Versorgungsspannung des Produkts und den anderen Schnittstellen getrennt. Baudraten von 1200 bis 115.200 werden unterstützt.

Die Buchse kombiniert eine Schnittstelle gemäß RS-232 und eine Schnittstelle gemäß RS-485. Die beiden Schnittstellen dürfen jedoch NICHT gleichzeitig verwendet werden!

Diese Kommunikationspartner müssen auf denselben Schnittstellentyp parametriert werden, da die Spannungspegel der beiden Typen NICHT kompatibel sind!

Tabelle 7: Pinbelegung X3

Kontakt	RS-232 (DCE)		RS-485	
	Signal	Beschreibung	Signal	Beschreibung
1	NC	Nicht belegt	NC	Nicht belegt
2	RxD (out)	Receive Data	NC	Nicht belegt
3	TxD (in)	Transmit Data	A (Tx/Rx+)	Transmit/receive data +
4	NC	Nicht belegt	NC	Nicht belegt
5	FB_GND	Masse	FB_GND	Masse
6	NC	Nicht belegt	FB_5V	Versorgung
7	NC	Nicht belegt	NC	Nicht belegt
8	NC	Nicht belegt	B (Tx/Rx−)	Transmit/receive data −
9	NC	Nicht belegt	NC	Nicht belegt
Gehäuse	Schirm	Schirmung	Schirm	Schirmung

ACHTUNG

Falsche Parametrierung kann zu Schäden am Kommunikationspartner führen!
Die Spannungspegel für RS-232 und RS-485 sind nicht kompatibel!
Wenn die Schnittstellen am Controller und am Kommunikationspartner unterschiedlich sind (RS-232 <> RS-485 oder RS-485 <> RS-232), kann dies zu Schäden an der Schnittstelle des Kommunikationspartners führen.
Achten Sie daher bei der Parametrierung des Controllers darauf, dass die Schnittstelle passend zum Kommunikationspartner eingestellt ist!

Zur Erhöhung der Störfestigkeit ist eine durchgehende Schirmung unbedingt erforderlich. Dazu ist das metallische Gehäuse der Buchse mit der Funktionserde verbunden.

Das angeschlossene Datenkabel muss geschirmt sein. Die verwendete Kabelschelle muss eine ausreichende Zugentlastung gewährleisten und gleichzeitig einen großflächigen Kontakt vom Schirm zum Gehäuse.

Die Datenrichtung der RS-232-Schnittstelle des Produkts entspricht dem Gerätetyp DCE.

4.3.4.1 Betrieb als RS-232-Schnittstelle

Abhängig vom Gerätetyp DTE (Data Terminal Equipment, z. B. PC) oder DCE (Data Communication Equipment, z. B. PFC, Modem) haben die RS-232-Signale unterschiedliche Datenrichtungen.

Tabelle 8: Funktion der RS-232-Signale bei DTE/DCE

Kontakt	Signal	Datenrichtung	
		DTE	DCE
2	RxD	Eingang	Ausgang
3	TxD	Ausgang	Eingang
5	FB_GND	---	---

Für eine DTE-zu-DCE-Verbindung werden die Signale direkt (1:1) verbunden.

Abbildung 5: Anschluss bei DTE-DCE-Verbindung (1:1)

Für eine DCE-zu-DCE-Verbindung werden die Signale gekreuzt (cross-over) verbunden.

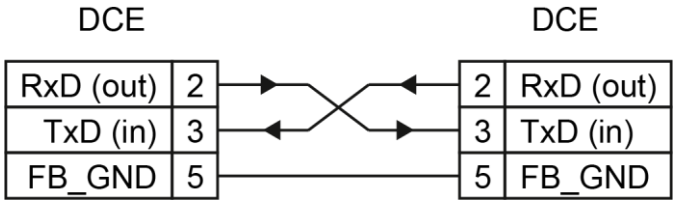

Abbildung 6: Anschluss bei DCE-DCE-Verbindung (cross-over)

4.3.4.2 Betrieb als RS-485-Schnittstelle

Um Reflektionen am Leitungsende zu minimieren, muss die RS-485-Leitung an beiden Enden mit einem Leitungsabschluss abgeschlossen werden. Falls erforderlich, kann je 1 Pull-Up- bzw. Pull-Down-Widerstand eingesetzt werden. Diese sorgen für einen definierten Pegel auf dem Bus, wenn kein Teilnehmer aktiv ist, d.h. alle Teilnehmer sich im „Tri-State“-Zustand befinden.

Hinweis

Busabschluss beachten!
Der RS-485-Bus muss an beiden Enden abgeschlossen sein!
Es dürfen nicht mehr als 2 Abschlüsse pro Bus eingesetzt werden!
In Stich- oder Abzweigstrecken darf kein Abschluss eingesetzt werden!
Stichleitungen müssen möglichst kurzgehalten werden!
Der Betrieb ohne korrekten Abschluss des RS-485-Netzes kann zu Übertragungsfehlern führen.

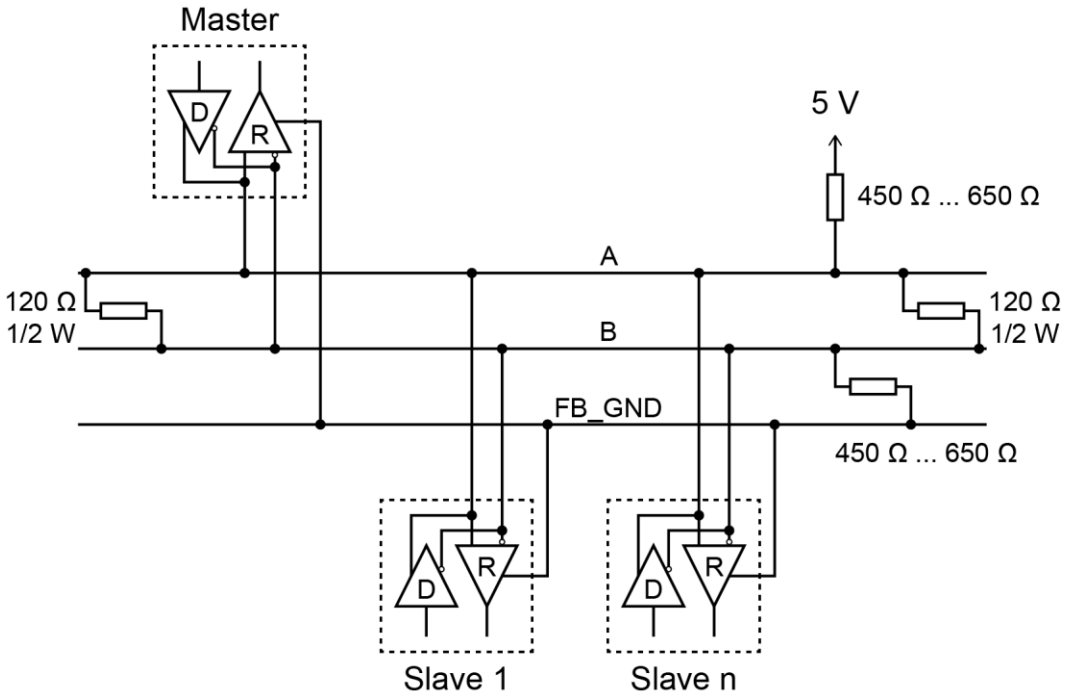

Abbildung 7: RS-485-Busabschluss

4.3.5 „X4“ – CAN-Schnittstelle

Diese Schnittstelle ist als D-Sub-9-Einbaustecker ausgeführt und ist galvanisch von der Versorgungsspannung des Gerätes und den anderen Schnittstellen

getrennt.
Die Schnittstelle entspricht ISO 11898-2.

Tabelle 9: Pinbelegung X4

Pin	Belegung
1	-
2	CAN-L (CAN data low)
3	GND (Bezugspotential 0 V bzw. Masse)
4	-
5	-
6	-
7	CAN-H (CAN data high)
8	-
9	-

Zur Erhöhung der Störfestigkeit ist eine durchgehende Schirmung unbedingt erforderlich. Das metallische Gehäuse des Steckers ist kapazitiv mit der Funktionserde verbunden.
Das angeschlossene Datenkabel muss geschirmt sein. Die verwendete Kabelschelle muss eine ausreichende Zugentlastung gewährleisten und gleichzeitig einen großflächigen Kontakt vom Schirm zum Gehäuse.

4.3.6 „X5“ – Versorgungsanschluss POWER

Schließen Sie die Versorgungsspannung an den Anschluss X5 an. Verwenden Sie dazu die mitgelieferte Federleiste 734-103 mit 3 CAGE CLAMP®-Anschlüssen.
Weitere Angaben zur Versorgung finden Sie im Kapitel „Technische Daten“.

Tabelle 10: Pinbelegung X5

Pin	Bezeichnung	Belegung
1	24VDC	Versorgungsspannung DC +24 V
2	GND	Bezugspotential 0 V (Masse)
3	FE	Funktionserde

4.3.7 „X6“ und „X7“ – USB-2.0-Schnittstellen

Diese USB-2.0-Host-Schnittstellen sind mit 4-poligen Typ-A-Buchsen ausgeführt. Jede Schnittstelle kann max. 500 mA liefern.

Die Anschlüsse entsprechen der USB-Spezifikation 2.0.

Hier können Tastaturen oder Mäuse als alternative Eingabegeräte oder auch bis zu 2 USB-Speicher angeschlossen werden. Diese USB-Geräte sind vor Power ON anzuschließen.

4.3.8 „X8“ – Lineout-Audioausgang (Kopfhörer)

Der Audioausgang ist eine 3-polige Stereoklinkenbuchse, 3,5 mm. Hier kann ein Kopfhörer oder eine kompatible Audioanlage angeschlossen werden, um z. B. akustische Warnsignale oder Sprachmeldungen auszugeben, die in der Steuerungsapplikation enthalten sind.

4.3.9 „X9“ – HDMI-Schnittstelle Typ A

Die Abkürzung HDMI steht für High Definition Multimedia Interface. Der HDMI-Anschluss ist ein Standardanschluss für die gleichzeitige Übertragung von Bild und Ton über nur ein Kabel. Über die HDMI-Schnittstelle kann das Produkt mit einem Monitor verbunden werden. Die FULL-HD-Auflösung (1920×1080) wird unterstützt.

Hinweis

HDMI-Schnittstelle für verschiedene Einsatzbereiche ausgelegt!
Im Wohn-, Geschäfts- und Gewerbebereich sowie in Kleinbetrieben ist die Verwendung der HDMI-Schnittstelle nicht zulässig.
Im Industriebereich ist die Verwendung der HDMI-Schnittstelle zulässig.

4.3.10 „X10“ – USB-C-Schnittstelle

Zur Inbetriebnahme und zu Service-Zwecken können Sie eine IP-Verbindung über die USB-Service-Schnittstelle aufbauen, siehe auch Kapitel „In Betrieb nehmen“ > „Einstellen einer IP-Adresse“ > „IP-Verbindung über USB“.

Die USB-Service-Schnittstelle ist als USB-C-Buchse ausgeführt. Die Schnittstelle unterstützt die USB-Spezifikation 2.0.

Der Controller stellt sich am Host-Gerät (PC) als Peripheriegerät im Device-Modus dar.

4.3.11 „X11“ – 4 Digitale Ein- und Ausgänge DIO

Vier digitale Anschlüsse, als Ein- oder Ausgänge konfigurierbar, dienen zum Anschluss von Aktoren und Sensoren.
Es wird ein 10-poliger *picoMAX*®-Steckverbinder verwendet mit 10 Push-in CAGE CLAMP®S-Anschlüssen (Federleiste 2091-1110).
Die Anschlüsse sind gemäß EN 61010-2-201 spezifiziert:
Gleichstromkreis, allgemeine Verwendung

Tabelle 11: Pinbelegung X11

CAGE CLAMP®	Bezeichnung	Belegung
1	GND	Bezugspotential 0 V (Masse)
2	DIO 0	Digitaler I/O 0
3	GND	Bezugspotential 0 V (Masse)
4	DIO 1	Digitaler I/O 1
5	GND	Bezugspotential 0 V (Masse)
6	DIO 2	Digitaler I/O 2
7	GND	Bezugspotential 0 V (Masse)
8	DIO 3	Digitaler I/O 3
9	GND	Bezugspotential 0 V (Masse)
10	24VDC	Einspeisung der Versorgungsspannung für digitale Ein- und Ausgänge

Die digitalen Ein-/Ausgänge sind galvanisch getrennt von der Versorgungsspannung des Produkts und von den anderen Schnittstellen.

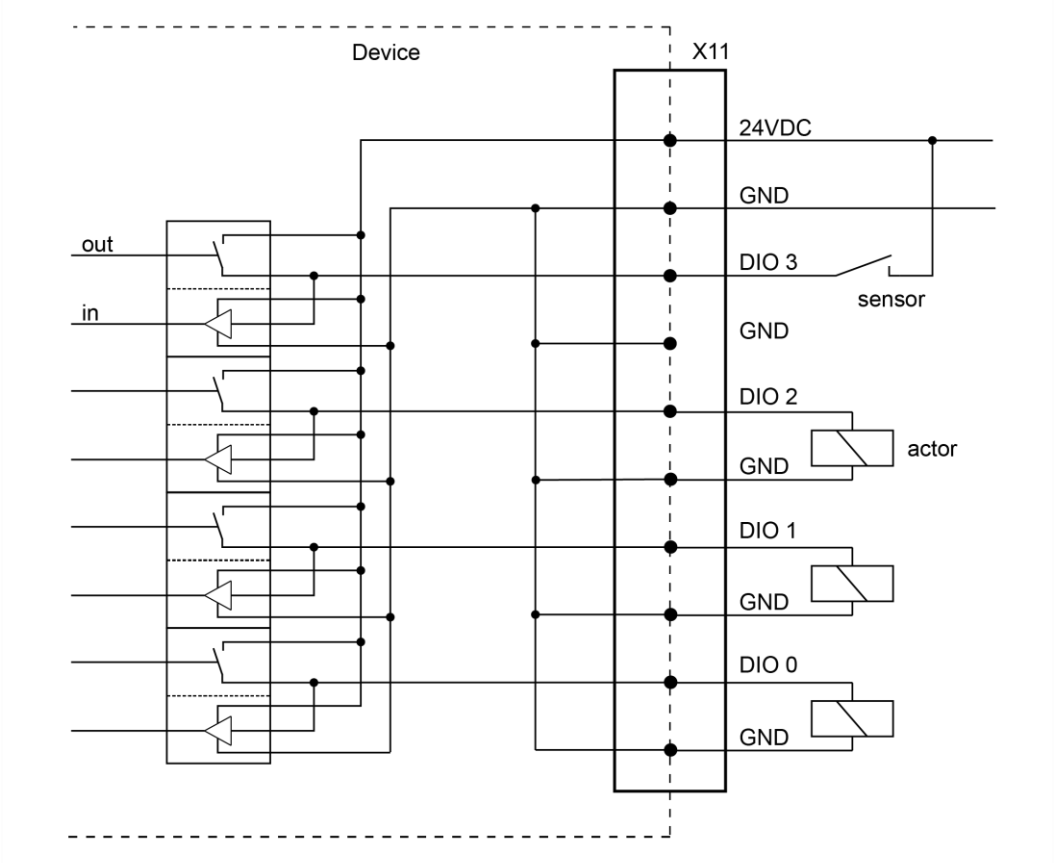

Abbildung 8: DIO-Anschlüsse X11 (Beispiel)

4.3.12 „µSD“ – Speicherkartensteckplatz

Das Produkt ist mit einem seitlich angebrachten Steckplatz für microSD- und microSDHC-Speicherkarten ausgestattet.

Hierfür können von WAGO getestete microSD- (max. 2 GB) und microSDHC-Karten (max. 32 GB) bezogen werden.

VORSICHT

Nur WAGO-Speicherkarten verwenden!
Bei Verwendung von Speicherkarten, die nicht von WAGO freigegeben wurden, kann keine Gewährleistung auf Funktion und Leistung gegeben werden!

Hinweis

Vorformatierung der Speicherkarten beachten!
Beachten Sie, dass Speicherkarten ≤ 2 GB oft mit dem Dateisystemtyp „FAT16“ formatiert sind und Sie maximal 512 Einträge in dem Root-Verzeichnis erzeugen können. Für mehr als 512 Einträge erzeugen Sie diese in einem Unterverzeichnis oder formatieren die Speicherkarte mit „FAT32“.

4.4 Echtzeituhr

Die Echtzeituhr (RTC= **R**eal **T**ime **C**lock) ist intern verbaut und nicht zugänglich. Sie dient ausschließlich zur internen Verwendung.

Abweichung/Genauigkeit

Die Abweichung ist kleiner ± 4 s/Tag bei einer Umgebungstemperatur von 25 °C.

Gangreserve

Die Uhr läuft nach Abschalten der Spannungsversorgung bei 25 °C mindestens 35 Tage weiter (entspricht 840 Stunden).
Bei Ausfall der Uhrzeit, nach mehr als 35 Tagen ohne Spannungsversorgung, erscheint ein Uhreinstelldialog, um die Uhrzeit neu einzugeben. Das Erscheinen des Dialogs kann konfiguriert ein- und ausgeschaltet werden.
Zur Pufferung ist keine Batterie vorhanden.

Auflösung

Die Auflösung der Uhr für Datum und Uhrzeit ist 1s.
Datum und Uhrzeit werden bereitgestellt und von der Applikation abgefragt.

4.5 Anzeigeelemente

4.5.1 Status-LED

Auf der linken Seite befinden sich 1 dreifarbige LED und 4 zweifarbige LEDs.

Die SYS-LED zeigt den Status an.

Tabelle 12: SYS-LED

Anzeige	Bedeutung
Grün leuchtend	Das Produkt ist betriebsbereit.
Rot blinkend	Ein Fehler liegt vor. Die betreffende Fehlermeldung wird angezeigt.
Blau blinkend	Ein Verbindungsfehler zum Controller liegt vor. Keine Kommunikation

Die RUN-LED zeigt den Programmstatus an.

Tabelle 13: RUN-LED

Anzeige	Bedeutung
Grün blinkend	Keine Applikation und kein Boot-Projekt geladen.
Grün leuchtend	CODESYS V3-Applikationen laufen.
Rot leuchtend	Alle CODESYS V3-Applikationen sind gestoppt.

Die CAN-LED zeigt den CANopen-Status an.

Tabelle 14: CAN-LED

Anzeige	Bedeutung
Grün leuchtend	Die CAN-Kommunikation läuft.
Rot leuchtend	Die CAN-Kommunikation ist gestört.

Zwei weitere Anwender-LEDs „H11“ und „H22“ sind für zukünftige Anwendungen vorgesehen.

4.6 Bedienelemente

Auf der linken Seite finden Sie den Betriebsartenschalter (BAS) und den Taster „CFG/RST“.

4.6.1 Betriebsartenschalter

Der Betriebsartenschalter hat folgende Stellungen:

Tabelle 15: Stellungen Betriebsartenschalter

Position	Bestätigung	Funktion
RESET	Tastend	**Reset Warmstart** oder **Reset Kaltstart** (abhängig von der Betätigungsdauer, siehe Kapitel „In Betrieb nehmen“ > „Reset-Funktionen auslösen“)
STOP	Rastend	**Stop** Alle CODESYS V3-Applikationen sind gestoppt
RUN	Rastend	**Normalbetrieb** CODESYS V3-Applikation läuft

In Verbindung mit dem Taster „CFG/RST“ kann ein „Factory-Reset“ ausgelöst werden. Siehe Kapitel „Service“ > „Factory-Reset“.

4.6.2 Taster „CFG/RST“

Der Taster „CFG/RST“ ist zur Vermeidung von Fehlbedienungen hinter einer Bohrung angebracht. Bei dem Taster handelt es sich um einen Kurzhubtaster mit einer geringen Betätigungskraft von 1,1 N … 2,1 N (110 gf … 210 gf). Der Taster ist mit einem geeigneten Gegenstand (z. B. einem Kugelschreiber) bedienbar.

Mit dem Taster „CFG/RST“ können Sie:

- die „Konfiguration mit dem WBM ändern“,
- die Werkseinstellungen wiederherstellen („Factory-Reset“).

Informationen zu den Funktionen finden Sie in den gleichnamigen Kapiteln weiter hinten in diesem Handbuch.

4.7 Schematisches Schaltbild

ACHTUNG

Keine USB-Geräte mit Verbindung zu Erde verwenden!
Die Abschirmungen der USB-Schnittstellen sind nicht direkt, sondern über Entstörkondensatoren mit Erde verbunden. An die USB-Schnittstellen dürfen nur Tastaturen, Mäuse und USB-Memory-Sticks angeschlossen werden. Geräte, die eine Verbindung zu Erde herstellen, wie z. B. Drucker, dürfen nicht angeschlossen werden, da dadurch die Entstörkondensatoren überbrückt werden und die Störfestigkeit sich reduziert.

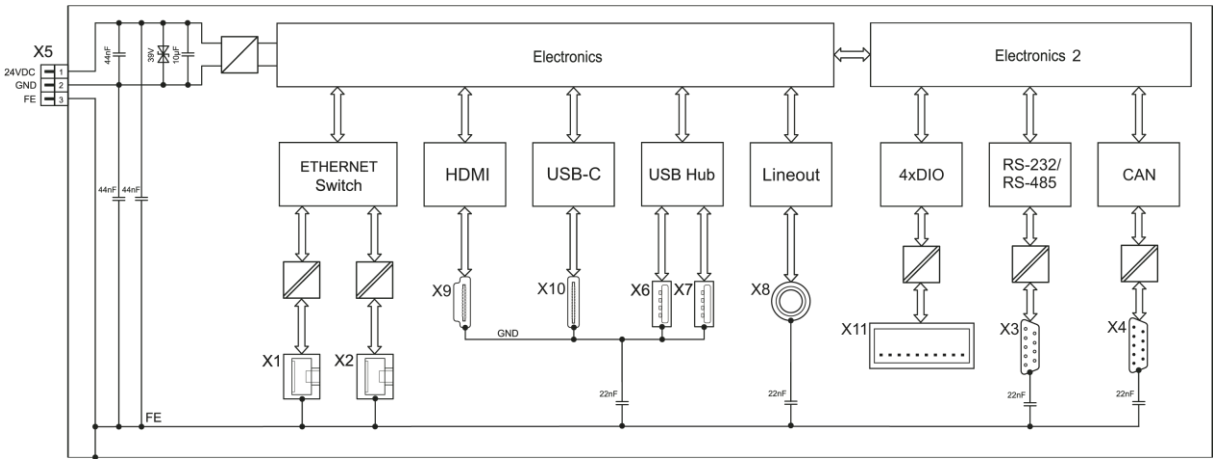

Abbildung 9: Schematisches Schaltbild

4.8 Technische Daten

4.8.1 Gerät

Tabelle 16: Technische Daten – Gerät

Gehäusematerial	Aluminium pulverbeschichtet
Abmessungen (Breite × Höhe × Einbautiefe)	65 × 123 × 115 mm
Befestigungsart	Tragschiene
Gewicht	835 g
IP-Schutzart	IP20
Schutzklasse	SK III
Überspannungskategorie	II
Verschmutzungsgrad	2

4.8.2 Klimatische Umgebungsbedingungen

Tabelle 17: Technische Daten – Klimatische Umgebungsbedingungen

Zulässige Betriebstemperatur	−20 ... +60 °C
Zulässige Lagerungstemperatur	−20 ... +80 °C
Relative Luftfeuchtigkeit (ohne Betauung)	90 %
Betriebshöhe	0 … 2000 m

4.8.3 Spannungsversorgung

Tabelle 18: Technische Daten – Spannungsversorgung

Spannung	SELV (Safety Extra Low Voltage – Sicherheitskleinspannung) Spannungsquelle, die die Anforderungen einer LPS (Limited Power Source) gemäß EN 60950-1 erfüllt DC 24 V (18 ... 31,2 V) mit Verpolungsschutz
Max. Stromaufnahme über den gesamten Spannungsbereich, ohne/mit externen USB-Geräten	120 mA / 390 mA
Max. Leistungsaufnahme über den gesamten Spannungsbereich, ohne/mit externen USB-Geräten	2,9 W / 9,4 W

4.8.4 Hardware

Tabelle 19: Technische Daten – Hardware

Prozessor	ARM® Cortex® A9 Quadcore 1.0 GHz
Externe Speichererweiterung („µSD“-Steckplatz)	microSD-Speicherkarte (max. 2 Gbyte) oder microSDHC-Speicherkarte (max. 32 Gbyte)
Hauptspeicher (RAM)	2 GB
Interner Speicher (Flash)	4 GB

4.8.5 Kommunikation

Tabelle 20: Technische Daten – Kommunikation

Feldbus	MODBUS TCP/UDP/RTU und CAN
Protokolle	ETHERNET TCP/IP, DHCP, DNS, FTP, FTPS, HTTP, HTTPS und SSH

4.8.6 Schnittstellen

Tabelle 21: Technische Daten – Schnittstellen

ETHERNET-Schnittstellen	2 × RJ-45-Buchse, mit Switch, 10/100 Mbit/s, Anschlussleitungen Twisted Pair SF-UTP, 100 Ohm, Kategorie 5e, Patch oder Crossover, max. 100 m lang
Serielle Schnittstelle RS-232/-485	1 × D-Sub-9-Einbaubuchse
CAN-Schnittstelle	1 × D-Sub-9-Einbaustecker
USB-Schnittstellen	2 × USB 2.0 Host (Typ A)-Buchse, 480 Mbit/s, Anschlussleitungen max. 3 m lang, Stromentnahme max. 2 × 500 mA 1 × USB OTG (Typ C)-Buchse
„µSD“- Steckplatz	Für microSD- und microSDHC-Speicherkarten
HDMI	1 × HDMI (Typ A)

4.8.7 Anschlüsse

Tabelle 22: Technische Daten – Anschlüsse

Versorgungsspannungs-einspeisung	3 × CAGE CLAMP®, Anschlussleitung max. 3 m bis zum Netzteil, Leiterquerschnitt 0,14 … 1,5 mm² / AWG 25 … 14, Abisolierlänge 7 mm / 0,28 inch, Leitermaterial Kupfer (Cu), Temperaturbeständigkeit der Leiter min. 75 °C
Audioausgang für Kopfhörer	3-polige Stereoklinkenbuchse, 3,5 mm, Kopfhörerausgang 62,5 mW an 16 Ohm, Frequenzbereich 20 … 20.000 Hz
4 digitale Ein- oder Ausgänge DIO	10 × Push-in CAGE CLAMP®, 4 x Eingänge gemäß IEC 61131-2 Typ1/Ausgänge als High-Side-Switch 24 V 0,5 A Leiterquerschnitt 0,2 … 1,5 mm² / AWG 24 … 14, Abisolierlänge 8 … 9 mm / 0,31 … 0,35 inch, Leitermaterial Kupfer (Cu), Temperaturbeständigkeit der Leiter min. 75 °C

4.9 Zulassungen

Folgende Zulassungen wurden für die Produkte erteilt:

Konformitätskennzeichnung

UK Conformity Assessed

cULus: UL61010-1, UL61010-2-201

Korea Certification: R-R-W43-EDGE752

Eurasian Conformity: EAC RU Д-DE.PA01.B.09690/21

Information

Weitere Informationen zu Zulassungen
Detaillierte Hinweise zu den Zulassungen finden Sie im Internet unter:
https://www.wago.com/de <Artikelnummer>

4.10 Normen und Richtlinien

Die Produkte erfüllen folgende EMV-Normen:

EMV CE-Störfestigkeit	EN 61000-6-2
EMV CE-Störaussendung	EN 61000-6-3

Hinweis

HDMI-Schnittstelle für verschiedene Einsatzbereiche ausgelegt!
Im Wohn-, Geschäfts- und Gewerbebereich sowie in Kleinbetrieben ist die Verwendung der HDMI-Schnittstelle nicht zulässig.
Im Industriebereich ist die Verwendung der HDMI-Schnittstelle zulässig.

5 Funktionen

Der Controller vereint HMI- und Steuerungsaufgaben, da er eine SPS gemäß IEC 61131-3 darstellt. Dazu können an den 4 digitalen I/Os 4 Aktoren bzw. Sensoren angeschlossen werden. Falls mehr benötigt werden, können über die Feldbus-Schnittstellen Feldbusknoten angebunden werden.

Die Inbetriebnahme erfolgt im Webbrowser mit der Software „Web-Based-Management WBM“. Anschließend wird im laufenden Betrieb der zu steuernden Anlage mit der CODESYS V3-Applikation die Target-Visualisierung über die HDMI-Schnittstelle angezeigt, die auf dem Engineering-PC mit CODESYS V3 programmiert wurde. Mittels des integrierten Webservers kann die Visualisierung auch weiteren Anzeigegeräten bereitgestellt werden.

Zur Kommunikation mit dem Engineering-PC wird ETHERNET verwendet. Die Kommunikation mit weiteren Controllern bzw. Koppler findet über ETHERNET oder einen Feldbus statt.

Hinweis

HDMI-Schnittstelle für verschiedene Einsatzbereiche ausgelegt!
Im Wohn-, Geschäfts- und Gewerbebereich sowie in Kleinbetrieben ist die Verwendung der HDMI-Schnittstelle nicht zulässig.
Im Industriebereich ist die Verwendung der HDMI-Schnittstelle zulässig.

5.1 Webbrowser

Der integrierte Webbrowser zeigt die Webseiten des Controllers/der Controller über die HDMI-Schnittstelle an.
Im WBM können bis zu 10 Controller konfiguriert werden. In der Auswahlliste „PLC-List“/„Browser Favorites“ können dann die Controller ausgewählt werden und deren Webvisualisierung direkt gestartet werden.

Der Webbrowser ist in der Lage, Webseiten über verschlüsselte Verbindungen (HTTPS) anzuzeigen.

Die virtuelle Tastatur öffnet sich automatisch bei Betätigen eines Eingabefeldes. Hierbei kann durch Drücken der Taste „Tastatur wechseln“ in verschiedene Ebenen (Buchstaben und Zahlen) umgeschaltet werden.
Innerhalb einer CODESYS-Visualisierung kann zwischen den Tastaturen „virtuelle Tastatur“ oder „CODESYS Numpad und Keypad“ gewählt werden.

Als Startseite kann Folgendes eingerichtet werden:

- das WBM
- die Auswahlliste „PLC-List“/„Browser Favorites“
- das direkte Starten der Webvisualisierung eines Controllers

Für das Einrichten der Startseite siehe Seite „Favorites“ im WBM.

5.2 Verbindungsüberwachung

Wird die Verbindung einer CODESYS-Visualisierung unterbrochen, erscheint eine Fehlermeldung im Browser. Dieser versucht automatisch, alle 10 Sekunden, die Verbindung wiederherzustellen (reconnect).

5.3 WBM für Konfigurieren/Parametrieren

Das Web-Based-Management (WBM) stellt Ihnen eine Oberfläche zur Konfiguration bzw. Parametrierung des Controllers zur Verfügung. Das WBM kann direkt auf dem Controller oder auch am Engineering-PC aufgerufen werden.

Eine detaillierte Beschreibung der bereitgestellten Bedienelemente und Funktionen lesen Sie im Kapitel „In Betrieb nehmen“.

5.4 Netzwerk

5.4.1 Schnittstellenkonfiguration

Die ETHERNET-Schnittstellen X1 und X2 sind mit einem internen 3-Port-Switch verbunden, dessen dritter Port mit der CPU verbunden ist. Der „Configuration Type“ ist im Auslieferungszustand auf „DHCP“ eingestellt. Die TCP/IP-Einstellungen wie die IP-Adresse oder die Subnetzmaske gelten sowohl für X1 als auch für X2.

5.4.1.1 Betrieb mit getrennten Netzwerk-Schnittstellen

Im Betrieb mit getrennten Netzwerk-Schnittstellen können die beiden ETHERNET-Schnittstellen separat konfiguriert und eingesetzt werden.
Zu beachten ist, dass die beiden Schnittstellen nach wie vor über die gleiche MAC-Adresse verfügen. Daher dürfen sie nicht im gleichen Netzsegment betrieben werden.

Beim Umschalten in den Betrieb mit getrennten Schnittstellen wird die Schnittstelle X2 mit den letzten für sie gültigen Einstellungswerten initialisiert. Die Verbindungen, die über die X1-Schnittstelle laufen, bleiben bestehen.

Bei Betrieb mit getrennten Schnittstellen und temporär fest eingestellter IP-Adresse kann das Gerät über die Schnittstelle X2 weiterhin über die regulär eingestellte IP-Adresse erreicht werden.

5.4.2 Netzwerksicherheit

5.4.2.1 Benutzer (User) und Passwörter

Es gibt mehrere 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!

5.4.2.2 Dienste und Benutzer

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

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

5.4.2.3 WBM-Benutzergruppe

Das WBM hat eine eigene Benutzerverwaltung. Die hier verwendeten Benutzer sind aus Sicherheitsgründen von den übrigen Benutzergruppen im System isoliert.
Bei der Erstinbetriebnahme werden Sie im WBM bei Anmeldung als Admin-Benutzer automatisch aufgefordert, ein neues Passwort zu vergeben.
Mit dieser Eingabe haben Sie aber noch nicht die Passwörter für die Linux®-Benutzer „root“ und „admin“ geändert!

Tabelle 23: WBM-Benutzer

Benutzer	Rechte	Standardpasswort
admin	Alle (administrator)	wago
user	Eingeschränkt	user

5.4.2.4 Linux®-Benutzergruppe

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

Die Passwörter für diese Benutzer sind über eine Terminalverbindung über SSH zu konfigurieren.

Tabelle 24: Linux®-Benutzer

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

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!

Beispiel

Die Änderung des voreingestellten Passwortes für den Linux®-Benutzer „root“ erfolgt mit dem Terminalprogramm PuTTY über ETHERNET mittels SSH.
Nach dem Starten der Software putty.exe erscheint „login as:“ Geben Sie hier „root“ ein und drücken Sie [**Enter**]. Sie werden nach dem Passwort gefragt. Geben Sie das voreingestellte Passwort „wago“ ein. Sie werden dann aufgefordert, ein neues Passwort zu vergeben „New password:“. Vergeben Sie ein individuelles Passwort, das einem entsprechenden Sicherheitsniveau entspricht und drücken Sie [**Enter**]. Sie werden aufgefordert, das Passwort zu wiederholen „Retype password:“. Geben Sie Ihr Passwort erneut ein und schließen Sie die Passwortänderung mit [**Enter**] ab.
Wiederholen Sie diesen Vorgang für die Anmeldung als Linux®-Benutzer „admin“.

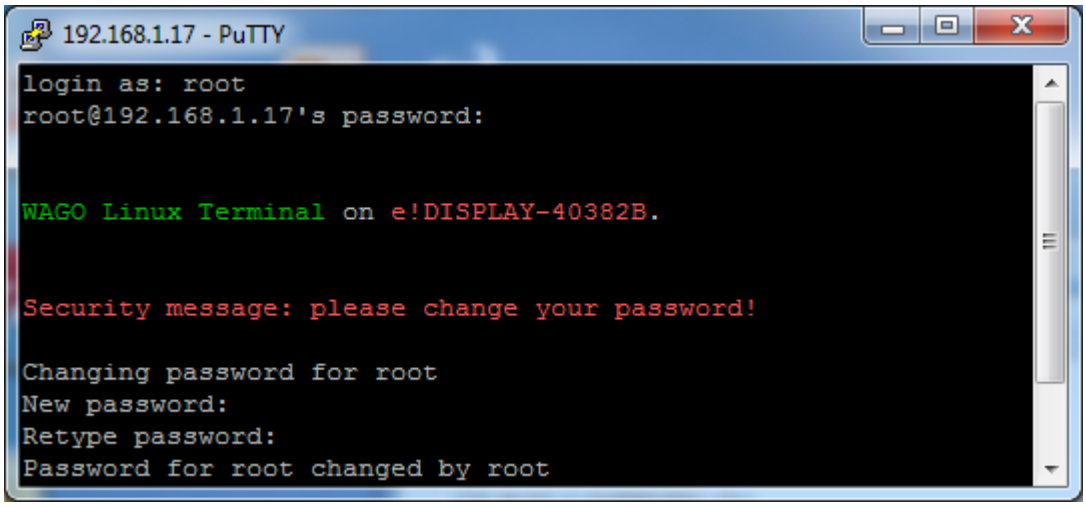

Abbildung 10: Beispiel Linux®-Passwort

5.4.2.5 SNMP-Benutzergruppe

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

5.4.2.6 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.

5.4.2.7 TLS-Verschlüsselung

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

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

Es sind die Einstellungen „Strong“ und „Standard“ möglich.
Mit der Einstellung „Strong“ erlaubt der Webserver nur die TLS-Version 1.2, 1.3 und starke Algorithmen. Ältere Software und ältere Betriebssysteme unterstützen eventuell TLS 1.2, TLS 1.3 und die Verschlüsselungsalgorithmen nicht.
Mit der Einstellung „Standard“ sind TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3 und auch kryptografische Verfahren erlaubt, die heute nicht mehr als sicher angesehen werden. Eine Verwendung wird nur für die Abwärtskompatibilität mit älteren Systemen empfohlen.

Information

Technische Richtlinie TR-02102 des BSI
Die Regeln für die Einstellung „Strong“ richten sich nach der technischen Richtlinie TR-02102 des Bundesamtes für Sicherheit in der Informationstechnik.
Die Richtlinie finden Sie im Internet unter: https://www.bsi.bund.de > „Publikationen“ > „Technische Richtlinien“.

Information

Leitfaden des BSI zur Migration auf TLS 1.2 bzw. TLS 1.3
Der Leitfaden des Bundesamtes für Sicherheit in der Informationstechnik zur Migration auf TLS 1.2 bzw. TLS 1.3 enthält „Kompatibilitätsmatrizen“, die darstellen, welche Software kompatibel zu TLS 1.2 bzw. TLS 1.3 ist.
Den Leitfaden finden Sie im Internet unter: https://www.bsi.bund.de > „Themen“ > „Standards und Kriterien“ > „Mindeststandards“.

5.4.3 Netzwerkkonfiguration

5.4.3.1 Hostname/Domainname

Ohne eine Konfiguration eines Hostnamens bekommt das Produkt einen Standardnamen, in den die letzten drei Werte der MAC-Adresse des Produkts eingehen. Dieser Name gilt, solange noch kein Hostname konfiguriert wurde bzw. kein Hostname per DHCP an das Produkt geliefert wurde (Zur Konfiguration siehe Kapitel „In Betrieb nehmen“ > „Im Web-Based-Management (WBM) 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. 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.

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.

5.4.3.2 Default-Gateways

Das Produkt erlaubt im Rahmen der TCP/IP-Konfiguration die Einstellung von zwei Default-Gateways. Ein Netzwerkteilnehmer sendet alle Netzwerk-Datenpakete für Systeme außerhalb seines lokalen Netzwerks an ein Default-Gateway. Dieses ist dafür zuständig, die Datenpakete geeignet weiterzuleiten, sodass sie das Zielsystem erreichen.

Den Default Gateways ist eine sogenannte Metrik zugewiesen, die angibt, mit welcher Zeitverzögerung, manchmal Kostenfaktor genannt, ein Datenpaket über das Gateway weitergeleitet werden kann. Sind nun mehrere Default-Gateways konfiguriert, sendet das Betriebssystem die Datenpakete an das Default-Gateway, welches mit der niedrigsten Metrik konfiguriert ist. Ist dieses Gateway nicht erreichbar, wird versucht, das Gateway mit der nächsthöheren Metrik zu erreichen. Haben mehrere der Gateways die gleiche Metrik, wird das Gateway zufällig bestimmt. Kann dieses Gateway das Datenpaket nicht senden, wird das Datenpaket parallel an alle anderen Gateways der gleichen Metrik verschickt.

Die Metrik der konfigurierten Default-Gateways kann für das Produkt vorgegeben werden. Der Standardwert für die Metrik ist 20. Neben den direkt konfigurierten Gateways können weitere Gateways durch DHCP-Antworten eingestellt werden, sodass in Summe mehr als zwei Gateways möglich sind. Alle per DHCP übergebenen Gateways bekommen unveränderbar eine Metrik von 10 zugeordnet. Damit werden im Standardfall die DHCP-Gateways wegen ihrer niedrigeren Metrik bevorzugt.

5.5 Speicherkartenfunktionen

Die Speicherkarte ist optional und dient als zusätzlicher Speicherbereich zu dem internen Speicher bzw. Laufwerk. Auf die Speicherkarte können Geräteeinstellungen sowie die Firmware des Produkts gespeichert werden.

5.5.1 Backup

Mit dieser 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.

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

5.5.2 Restore

Mit dieser 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.

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

Hinweis

Bei Parameteränderungen führt das Gerät einen Neustart durch!
Beachten Sie, dass das Gerät zur Übernahme der Daten einen Neustart durchführt, wenn Parameter mit anderen Einstellungen von der Speicherkarte überschrieben 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.

5.5.3 Create Image

Mit dieser WBM-Funktion kann eine bootfähige Kopie des aktuell gebooteten Systems erstellt werden. D.h. wurde das Produkt vom internen Flash gestartet, so wird mit der Funktion „Create Image“ eine Kopie auf die Speicherkarte geschrieben. Wurde das Produkt von der Speicherkarte gestartet, so wird mit der eine Kopie auf das interne Flash abgelegt. Dabei wird das vorhandene Image gelöscht.

5.6 Nachladen von Software

Das Produkt bietet die Möglichkeit, einzelne Softwarepakete nachzuinstallieren bzw. zu aktualisieren. Die Softwarepakete werden von WAGO bereitgestellt. Sie können diese per WBM von Ihrem PC installieren. Siehe auch WBM-Seite „Software Uploads“.

5.7 Booten

Startverhalten

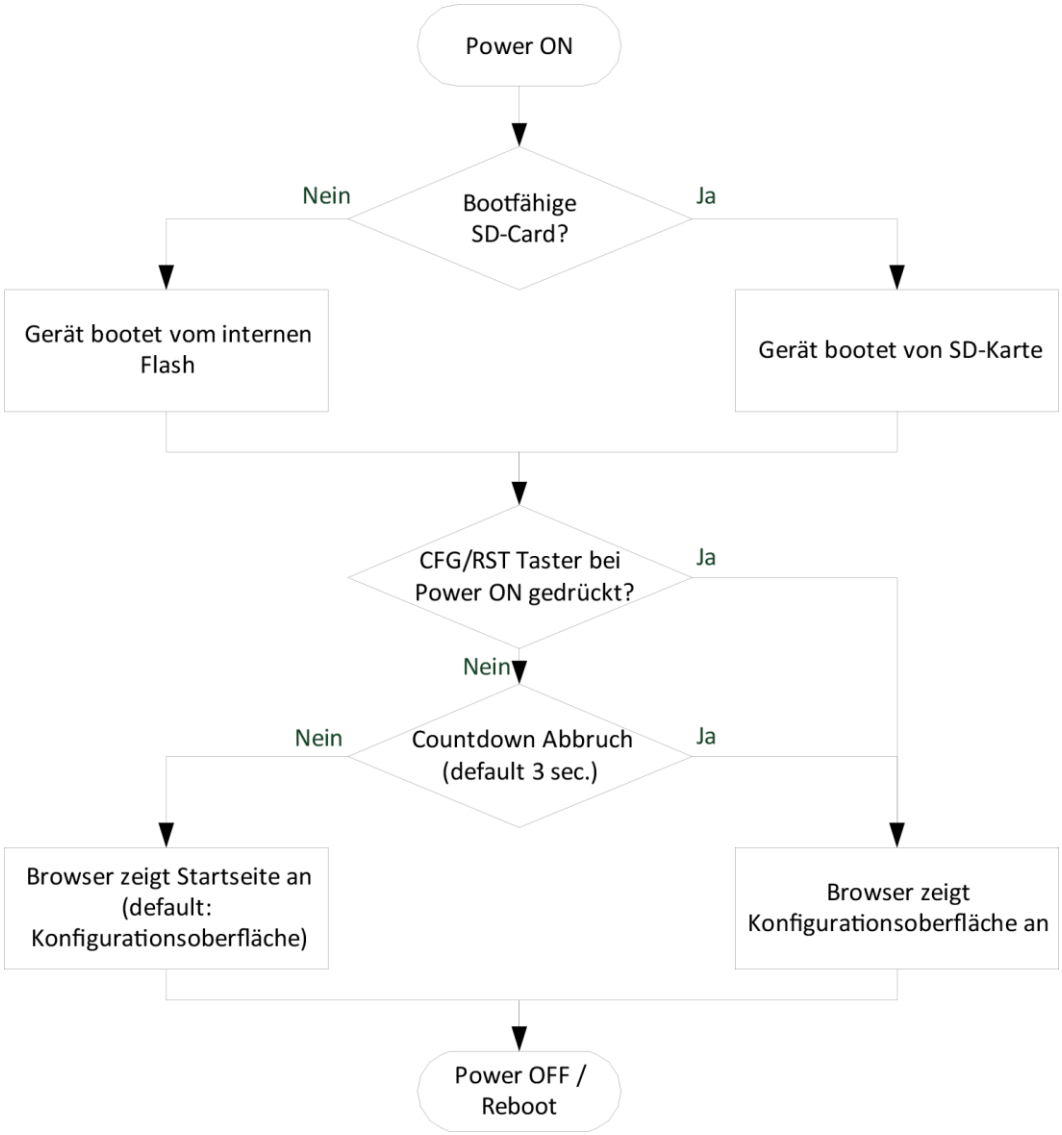

Abbildung 11: Startverhalten

Browser

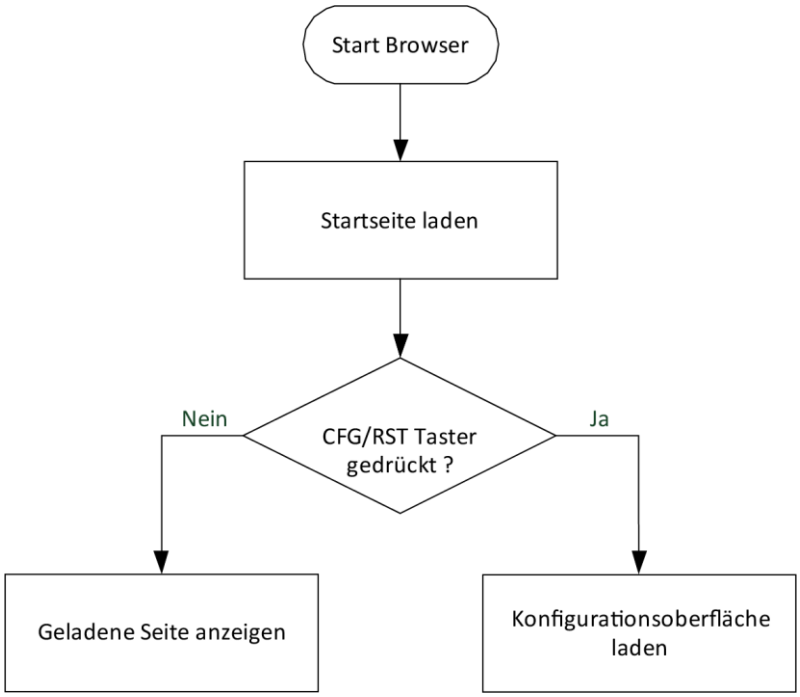

Abbildung 12: Browserablauf

Taster „CFG/RST“

Eine Betätigung des Tasters „CFG/RST“ zur Laufzeit öffnet das WBM. Drücken beim Starten (Power ON) des Produkts unterbindet den normalen Autostart und es startet nur das WBM. Es werden keine Änderungen an den Einstellungen durch den Taster vorgenommen.

5.8 Lizenzpflichtige Softwarekomponenten

Für das Produkt sind für das Laufzeitsystem CODESYS V3 Softwarekomponenten erhältlich, die einer Lizenzprüfung unterliegen (Runtime-Lizenzen).

Die Lizenzierung kann mit Add-on Licensing durchgeführt werden.

Für den produktiven, zeitlich unbegrenzten Einsatz einer lizenzpflichtigen Softwarekomponente wird ein Lizenzschlüssel benötigt. Auch ohne Lizenzschlüssel ist die Softwarekomponente 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.

Der Lizenzstatus („Testzeit läuft“ oder „Testzeit abgelaufen“) wird vom Controller über die SYS-LED angezeigt.

6 Montieren

ESD

Elektrostatische Entladung vermeiden!
In den Geräten sind elektronische Komponenten integriert, die Sie durch elektrostatische Entladung bei Berührung zerstören können. Beachten Sie die Sicherheitsmaßnahmen gegen elektrostatische Entladung gemäß IEC 61340-5-1/-3. Achten Sie beim Umgang mit den Geräten auf gute Erdung der Umgebung (Personen, Arbeitsplatz und Verpackung).

ACHTUNG

Belüftungsöffnungen nicht abdecken!
Zur Gewährleistung einer ausreichenden Luftzirkulation müssen die Belüftungsöffnungen freigehalten werden.
Halten Sie an den Belüftungsöffnungen einen Abstand von mind. 100 mm zu angrenzenden Oberflächen ein.

Hinweis

Direkte Lichteinstrahlung vermeiden!
Positionieren Sie das Produkt so, dass es keiner direkten starken Lichtquelle wie z. B. Sonnenlicht ausgesetzt ist!

6.1 Aufbaurichtlinien und Normen

DIN 60204	Elektrische Ausrüstung von Maschinen
DIN EN 50178	Ausrüstung von Starkstromanlagen mit elektronischen Betriebsmitteln (Ersatz für VDE 0160)
EN 60439	Niederspannungsschaltgerätekombinationen

6.2 Einbaulagen

Als Nenneinbaulage gilt: Frontseite vorn, Beschriftung lesbar, Belüftungsöffnungen oben und unten.

Alternativ kann das Produkt auch waagerecht montiert werden, sodass die Anschlüsse nach unten zeigen. Dafür wird der Tragschienenadapter auf der Rückseite entfernt und seitlich angebracht.

Das Produkt darf nicht direkt angereiht betrieben werden! Zu aktiven Nachbarn (gleichwertiges Produkt unter Volllast) muss ein Abstand von mindestens 12 mm eingehalten werden; zu passiven Nachbarn (keine aktive Wärmeerzeugung) ein Abstand von mindestens 6 mm.

6.3 Montage auf Tragschiene

Montieren Sie das Produkt durch Aufrasten auf die Tragschiene 35 gemäß EN 60715:

1. Setzen Sie das Produkt mit der Tragschienenführung an die Oberkante der Tragschiene ein.

2. Drücken Sie das Produkt in Richtung Tragschiene und rasten Sie das Produkt bei gleichzeitigem Zug an der Lasche auf.

3. Zur sicheren Fixierung auf der Tragschiene setzen Sie vor und nach dem Produkt je eine Endklammer (z. B. Artikelnr. 249-197).

7 Anschließen

7.1 Erden

Die Erdung erfolgt über den Anschluss X5.
Verwenden Sie dazu den mitgelieferten Stecker (Federleiste 734-103) mit 3 CAGE CLAMP®-Anschlüssen. Öffnen Sie den CAGE CLAMP®-Anschluss Nr. 3 mit einem Betätigungswerkzeug. Führen Sie einen 7 mm abisolierten Leiter mit max. 1,5 mm² ein und ziehen Sie das Betätigungswerkzeug wieder heraus. Stecken Sie den Stecker auf den Anschluss X5 und prüfen Sie anschließend die feste Klemmverbindung.

7.2 Geräte anschließen

Der elektrische Anschluss der Peripheriegeräte erfolgt über die Schnittstellen auf der Ober-und Vorderseite.

Die **ETHERNET-Schnittstellen** dienen der Anbindung an ein LAN bzw. an das Internet zur Kommunikation mit dem Controller. Es können sowohl Crossover- als auch Patch-Kabel Kategorie 5e verwendet werden.

Die **USB-2.0-Schnittstellen** dienen dem Anschluss von Tastatur oder Maus als alternative Eingabegeräte. Es können auch maximal 2 USB-Speicher angeschlossen werden. Da auf dem Markt eine große Vielfalt an USB-Geräten besteht, kann keine Garantie für die Funktion der einzelnen Geräte gegeben werden.
USB-/HDMI-Geräte sind vor Power ON anzuschließen, da sie nicht hot-plug-fähig sind.

ACHTUNG

Keine USB-Geräte mit Verbindung zu Erde verwenden!
Die Abschirmungen der USB-Schnittstellen sind nicht direkt, sondern über Entstörkondensatoren mit Erde verbunden. An USB-Schnittstellen dürfen nur Tastaturen, Mäuse und Memory-Sticks angeschlossen werden. Geräte, die eine Verbindung zu Erde herstellen, wie z. B. Drucker, dürfen nicht angeschlossen werden, da dadurch die Entstörkondensatoren überbrückt werden und die Störfestigkeit sich reduziert.

ACHTUNG

HDMI nur im industriellen Umfeld!
Die HDMI-Schnittstelle darf nur im industriellen Umfeld eingesetzt werden. Schließen Sie den HDMI-Port im Wohn-, Geschäfts- und Gewerbebereich sowie in Kleinbetrieben nicht an.

microSD-Speicherkarten werden so weit in den Steckplatz gesteckt, bis sie hörbar einrasten. Der Steckplatz kann dann zum Schutz verplombt werden. Zum Entfernen drücken Sie die Karte weiter herunter, bis sich die Arretierung löst. Jetzt kann die Karte herausgenommen werden.

Wenn Ihre Applikation akustische Signale/Warnungen enthält, können Sie in die **Audioausgangsbuchse** den 3,5 mm-Stereoklinkenstecker eines Kopfhörers o. ä. Audiosystems einstecken.

Weitere Angaben zu den Schnittstellen finden Sie im Kapitel „Eigenschaften“ > „Anschlüsse“ und „Technische Daten“.

7.3 Versorgungsspannung anschließen

Die Versorgungsspannung schließen Sie an den Anschluss X5, Pin 1 (+) und 2 (−) an.
Verwenden Sie dazu ebenfalls den mitgelieferten Stecker (Federleiste 734-103).

8 In Betrieb nehmen

8.1 Einschalten

Das Produkt hat keinen Ein-/Ausschalter und wird daher zusammen mit Ihrer Anlage eingeschaltet.

Nach dem Hochfahren des Systems gelangen Sie, je nach Einstellung, automatisch oder manuell über die HDMI-Schnittstelle zum WBM, zur „PLC-List“/„Browser Favorites“ oder zu einem ausgewählten Controller. Sie können die automatische Weiterleitung unterbrechen und zu einem Auswahlmenü gelangen, wenn Sie den dargestellten Countdown durch Klicken unterbrechen.

8.2 Log-in

Bevor die Oberfläche des WBM angezeigt werden kann, werden Sie aufgefordert, sich mit Benutzernamen und Passwort anzumelden. Wenn Sie das WBM zum ersten Mal starten, müssen Sie das Initialpasswort verwenden. Sie können sich als „administrator“ oder „user“ anmelden. Den Benutzergruppen stehen unterschiedliche Funktionalitäten zur Verfügung. Siehe „Im Web-Based-Management (WBM) konfigurieren > Benutzerverwaltung des WBM“ und „Im Web-Based-Management (WBM) konfigurieren > Zugriffsrechte“.

8.3 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.

8.4 Einstellen einer IP-Adresse

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

Tabelle 25: Voreingestellte IP-Adressierungen der Ethernet-Schnittstellen

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

Damit ein PC und der Controller miteinander kommunizieren können, passen Sie mit einem der vorhandenen Konfigurationswerkzeuge (z. B. WBM oder WAGO Ethernet Settings) die IP-Adressierung an Ihre Systemstruktur an (siehe Kapitel „Konfigurieren“).

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

- Die IP-Adresse des Host-PCs lautet **192.168.1.2**.
- Controller 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 Controllers müssen bei einer Subnetzmaske von **255.255.255.0** übereinstimmen, damit sich beide im gleichen Subnetz befinden.

Tabelle 26: Netzmaske 255.255.255.0

Host-PC	Subnetzadressraum für den Controller
192.168.1.2	**192.168.1**.1 oder **192.168.1**.3 … **192.168.1**.254

8.4.1 IP-Verbindung über USB

1. Verbinden Sie den Controller über die USB-Service-Schnittstelle und ein geeignetes USB-C-Servicekabel 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 192.168.42.42 auf.
   Das Web-Based-Management des Controllers wird geöffnet. Sie können damit alle erforderlichen Einstellungen am Controller durchführen.

8.4.2 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 ein geeignetes USB-C-Servicekabel oder ggf. das IP-Netzwerk verwenden.

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

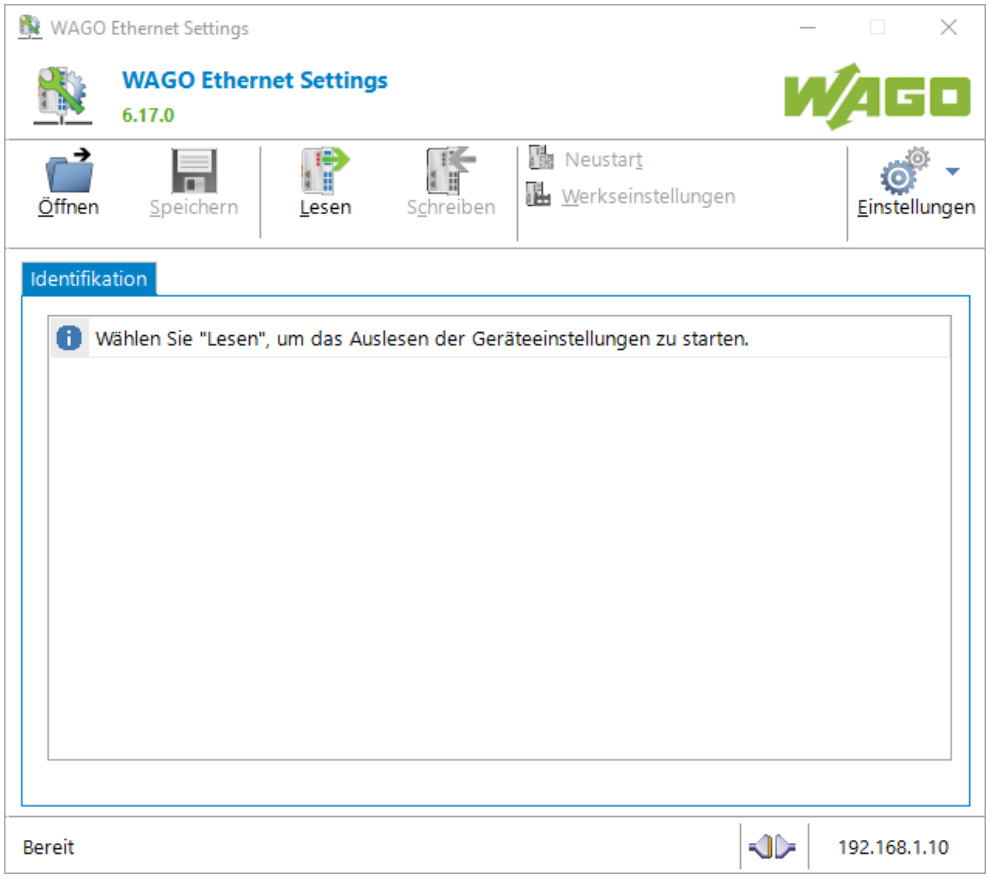

Abbildung 13: „WAGO Ethernet Settings“ – Startbildschirm (Beispiel)

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

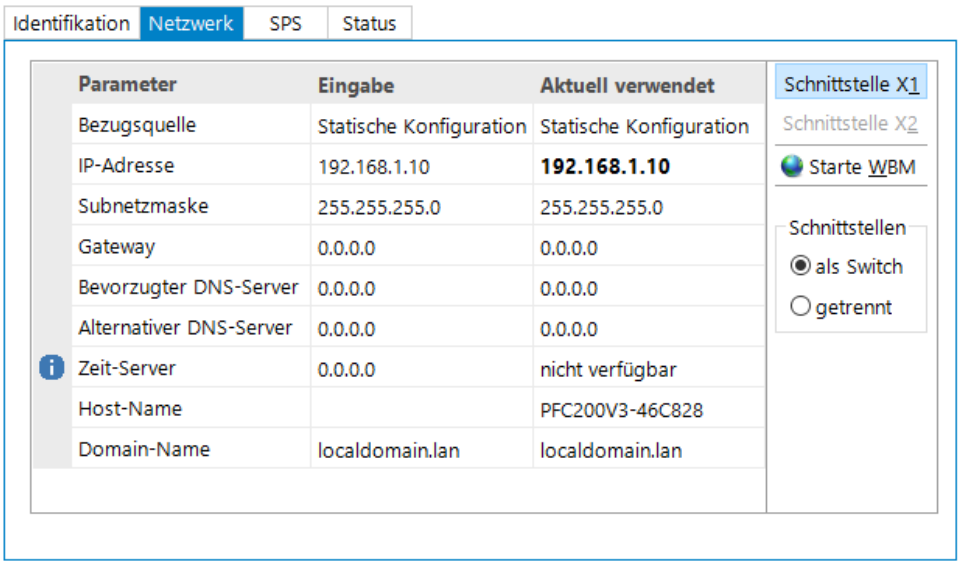

Abbildung 14: „WAGO Ethernet Settings“ – Register Netzwerk (Beispiel)

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.

8.4.3 Temporär eine feste IP-Adresse einstellen

Mit diesem Vorgang wird die IP-Adresse für die Schnittstelle X1 temporär auf die feste Adresse „192.168.1.17“ eingestellt.
Bei eingeschaltetem Switch wird die feste Adresse auch für die Schnittstelle X2 verwendet.
Bei ausgeschaltetem Switch wird die ursprüngliche Adresseinstellung für die Schnittstelle X2 nicht verändert.
Es wird kein Reset durchgeführt.

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

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

2. Betätigen Sie den Taster „CFG/RST“ länger als 8 Sekunden.

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

Um die Einstellung wieder aufzuheben, gehen Sie folgendermaßen vor:

- Führen Sie einen Software-Reset durch oder
- Schalten Sie den Controller aus und wieder ein.

8.4.4 Einstellen der 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 Netzwerkkabel.
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.

8.4.5 Zuweisen einer IP-Adresse mittels 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 angebundenen 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 Gerätes ist auf dem seitlich am Gerät angebrachten Etikett aufgedruckt.

Im nachfolgenden Beispiel ist die entsprechende Ausgabe von „Open DHCP“ zu sehen.

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

Abbildung 15: „Open DHCP, Beispielbild“

Im abgebildeten Beispiel lautet das Präfix „Host“ und die MAC-ID lautet „00:30:de:46:68:98“.

Der Hostname ist damit „Host0030de466898“.

8.5 Reset-Funktionen auslösen

Mit dem Betriebsartenschalter und dem Taster „CFG/RST“ können Sie verschiedene Reset-Funktionen auslösen.

8.5.1 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.

8.5.2 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“.

Um einen Kaltstart-Reset durchzuführen, bringen Sie den Betriebsartenschalter in die Reset-Position und halten ihn dort länger als 7 Sekunden.
Die Ausführung wird nach Ablauf der 7 Sekunden durch ein längeres Erlöschen der roten „RUN“-LED signalisiert. Lassen Sie den Betriebsartenschalter anschließend wieder los.

8.5.3 Software-Reset (Neustart)

Bei einem Software-Reset wird der Controller neu gestartet.

Um einen Software-Reset durchzuführen, bringen Sie den Betriebsartenschalter in die RUN- oder STOP-Position und betätigen Sie den Taster „CFG/RST“ länger als 1 Sekunde aber kürzer als 8 Sekunden.

Die Ausführung wird durch ein kurzes rotes und anschließend weißes Aufleuchten der SYS-LED signalisiert. Nach einigen weiteren Sekunden signalisiert die SYS-LED den erfolgreichen Bootvorgang des Controllers.

8.5.4 Factory-Reset

ACHTUNG

Controller nicht ausschalten!
Durch eine Unterbrechung des Factory-Reset-Vorgangs kann der Controller beschädigt werden.
Schalten Sie den Controller während des Factory-Reset-Vorgangs nicht aus und unterbrechen Sie nicht die Spannungsversorgung!

Hinweis

Alle Parameter und Passwörter werden überschrieben!
Mit dem Factory-Reset werden alle Parameter und Passwörter des Controllers überschrieben.
Gespeicherte Boot-Projekte einschließlich vorhandener Webvisualisierungsdaten werden gelöscht.
Nachinstallierte Firmwarefunktionen werden nicht überschrieben.
Bei Rückfragen wenden Sie sich an den WAGO Support.

Nach dem Factory-Reset wird der Controller neu gestartet.

Wenn Sie für den Controller einen Factory-Reset durchführen möchten, gehen Sie folgendermaßen vor:

1. Betätigen Sie den Reset-Taster (CFG/RST).
2. Bringen Sie den Betriebsartenschalter in die Position „RESET“.
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.

Hinweis

Reset-Vorgang nicht unterbrechen!
Wenn Sie den Reset-Taster (CFG/RST) zu früh loslassen, dann startet der Controller neu, ohne den Factory-Reset durchzuführen.

8.6 Im Web-Based-Management (WBM) konfigurieren

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 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 dazu Kapitel „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 („Fix IP Address“-Modus, siehe Kapitel „In Betrieb nehmen“ > … > „Temporär eine feste IP-Adresse einstellen“).

Hinweis

Auslastung durch CODESYS Programm berücksichtigen
Wenn der Controller durch ein CODESYS Programm ausgelastet ist, kann dies zu einer verlangsamten Verarbeitung im WBM führen. Unter Umständen werden deshalb Time-out-Fehler gemeldet. Es ist deshalb sinnvoll, vor umfangreichen Konfigurationen über das WBM die CODESYS Applikation zu stoppen.

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

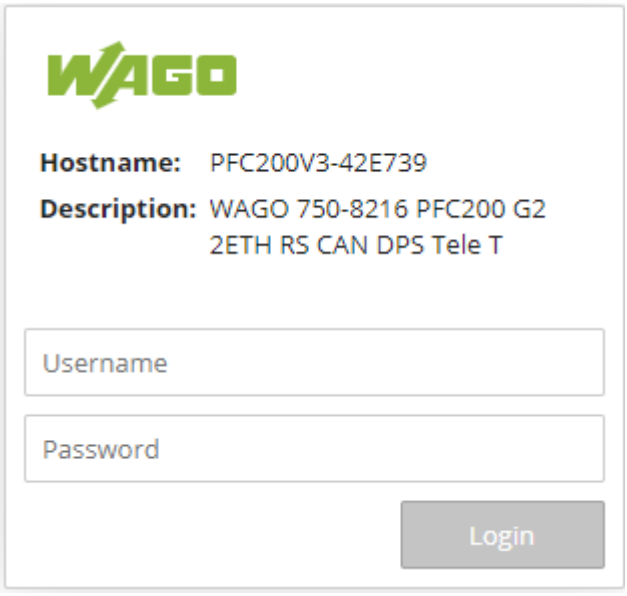

Abbildung 16: Authentifizierung eingeben (Beispiel)

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 Log-in-Session abzuspeichern.

8.6.1 Benutzerverwaltung des WBM

Um Einstellungen nur durch einen ausgewählten Personenkreis zu erlauben, begrenzen Sie über die Benutzerverwaltung den Zugriff auf die Funktionen des WBM.

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!

Solange Sie die Passwörter nicht ändern, wird nach dem Einloggen bei jeder aufgerufenen WBM-Seite ein entsprechender Warnhinweis erscheinen.

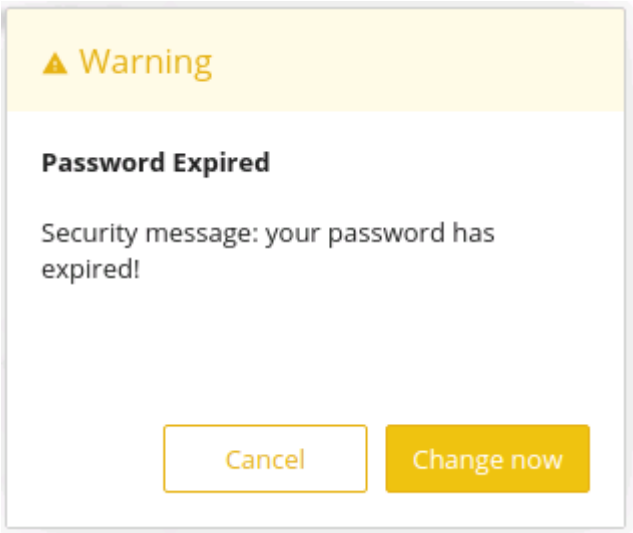

Abbildung 17: Passworterinnerung

Wenn Sie auf die Schaltfläche **[Change now]** klicken, werden Sie direkt auf die WBM-Seite weitergeleitet, auf der Sie das Passwort ändern können.

Tabelle 27: Benutzereinstellungen im Auslieferungszustand

Benutzer	Rechte	Standardpasswort
root	Alle (administrator)	wago
admin	Alle (administrator)	wago
user	Eingeschränkt	user

Hinweis

Übergreifende Rechte der WBM-Benutzer
Die WBM-Benutzer „root“, „admin“ und „user“ besitzen über das WBM hinausgehende Rechte, um das System zu konfigurieren und Software zu installieren.

Die Benutzerverwaltung für die Steuerungsanwendungen wird separat angelegt und verwaltet.

Die Zugriffsrechte für die WBM-Seiten sind in der nachfolgenden Tabelle dargestellt.

Der Benutzer „root“ hat die gleichen Rechte wie der Benutzer „admin“ und ist daher nicht separat aufgelistet.

Tabelle 28: Zugriffsrechte für die WBM-Seiten

Register/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	Tademarks Information	user
WBM Version	WBM Version Info	user
Configuration		
PLC Runtime	PLC Runtime Configuration	user
Networking		
TCP/IP Configuration	TCP/IP Configuration	user
Ethernet Configuration	Ethernet Configuration	user
Host/Domain Name	Configuration of Host and Domain Name	user
Routing	Routing	user
STP/RSTP	Spanning Tree Protocol	user
Clock	Clock Settings	user
Administration		
Serial Interface	Configuration of Serial Interface RS232/RS485	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
DHCP Server	DHCP Server Configuration	admin
DNS	Configuration of DNS Service	admin
Cloud Connectivity		

Tabelle 28: Zugriffsrechte für die WBM-Seiten

Register/Navigation	WBM-Seitentitel	Benutzer
Status	Overview	admin
Connection 1	Configuration	admin
Connection 2	Configuration	admin
SNMP		
General Configuration	Configuration of general SNMP parameters	admin
SNMP v1/v2c	Configuration of SNMP v1/v2c parameters	admin
SNMP v3	Configuration of SNMP v3 Users	admin
Browser Settings		
Favorites	Favorites	user
Autostart	Autostart	user
Monitoring	Monitoring	user
Browser Security	Browser Security	user
Commissioning	Commissioning Settings	admin
Docker	Docker Settings	admin
Display		
Font Upload	Fonts	user
Display Orientation	Display Orientation	user
Screensaver	Screensaver	user
Users	WBM User Configuration	user
Fieldbus		
OPC UA	OPC UA Configuration	admin
BACnet		
Status	BACnet Status	admin
Configuration	BACnet Configuration	admin
Data Link	BACnet Data Link	admin
Storage Location	BACnet Storage Location	admin
Security		
OpenVPN / IPsec	OpenVPN / IPsec Configuration	admin
Firewall		
General Configuration	General Firewall Configuration	admin
Interface Configuration	Interface Configuration	admin
MAC Address Filter	Configuration of MAC Address Filter	admin
User Filter	Configuration of User Filter	admin
Certificates	Certificates	admin
Boot Mode	Boot mode configuration	admin
TLS	Security Settings	admin
Integrity	Advanced Intrusion Detection Environment (AIDE)	admin

Tabelle 28: Zugriffsrechte für die WBM-Seiten

Register/Navigation		WBM-Seitentitel	Benutzer
	WAGO Device Access	WAGO Device Access	admin
Diagnostic			
	Log Message	Log Message Viewer	user
	Download	Download	admin
	Network Capture	Network Capture	admin

8.6.2 Allgemeine Seiteninformationen

In der Eingabezeile des Browserfensters wird die IP-Adresse des angesprochenen Gerätes angezeigt.

Die WBM-Seiten werden erst nach der Anmeldung angezeigt. Zur Anmeldung geben Sie im Anmeldefenster Benutzername und Passwort ein und klicken Sie auf die Schaltfläche **[Login]**.

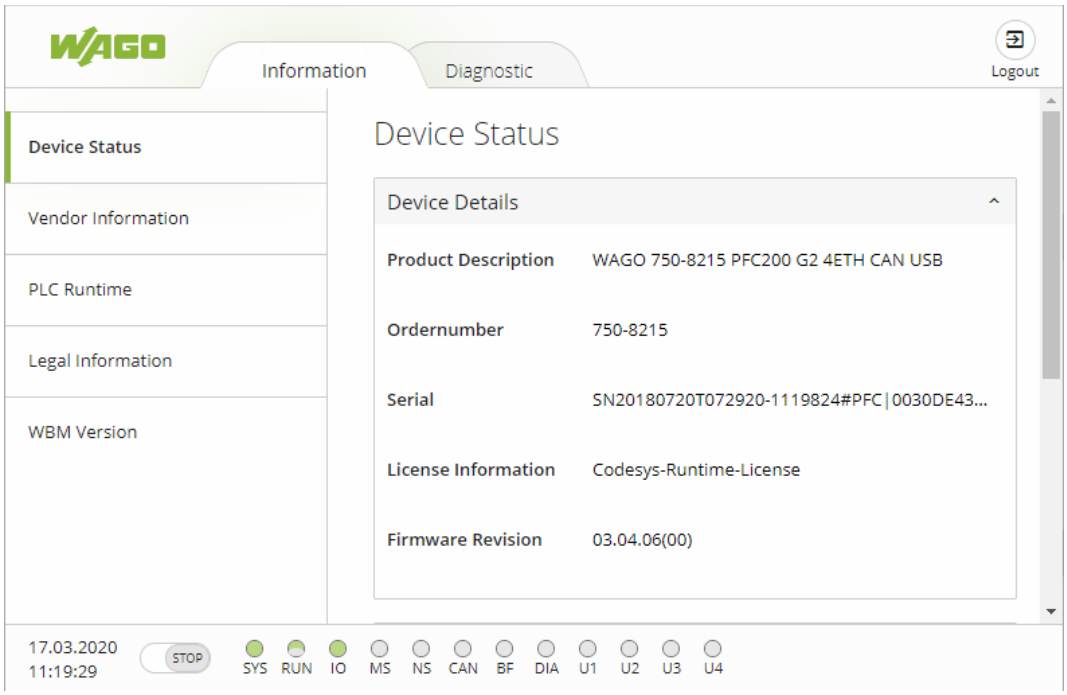

Abbildung 18: WBM-Browserfenster (Beispiel)

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.

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

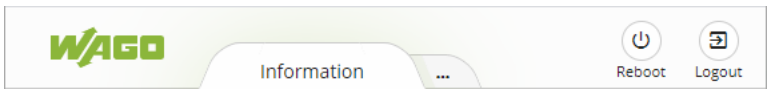

Abbildung 19: WBM-Kopfzeile mit nicht darstellbaren Registerkarten (Beispiel)

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.

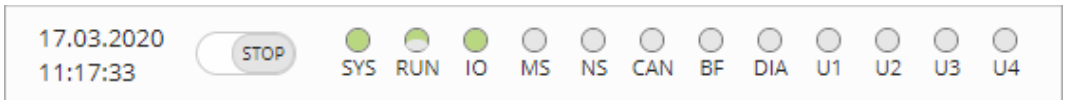

Abbildung 20: WBM-Statuszeile (Beispiel)

- 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, ...) beschriftet und die Zustände werden über eine Grafik symbolisiert.
  Es sind folgende Darstellungen möglich:

  - grau: Die LED ist aus.
  - 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 sequentiell 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 Gerät. 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.

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.

Eine Beschreibung der WBM-Seiten und der jeweiligen Parameter finden Sie im Anhang im Abschnitt „Konfigurationsdialoge“ > „Web-Based-Management (WBM)“.

8.6.3 Reboot-Funktion

Klicken Sie die Schaltfläche **[Reboot]**. Um den Neustart zu bestätigen, klicken Sie **[Reboot]**. Um einen Neustart abzubrechen, klicken Sie **[Cancel]**.

9 Laufzeitumgebung CODESYS V3

9.1 Grundlegende Hinweise

Information

Weitere Information
Informationen zur Installation, Inbetriebnahme und Programmierung finden Sie in der Dokumentation zu CODESYS V3.

9.2 CODESYS V3-Prioritäten

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

Tabelle 29: CODESYS V3-Prioritäten

Scheduler	Aufgabe	Linux®-Priorität	IEC-Priorität	Bemerkung
Preemptives Scheduling - Echtzeit-bereich	Lokal- oder Feldbus - HIGH	-95 … -86		Lokalbus (-88)
	Betriebsarten-schalter-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-Echtzeit-bereich	CODESYS Kommunikation	Back-ground (20)		Kommunikation mit der CODESYS Entwicklungs-umgebung
	Zyklische, ereignisgesteuerte und freilaufende IEC-Task		15	U.a. Standardpriorität der Visualisierungstask

9.3 Speicherbereiche unter CODESYS V3

Die Speicherbereiche haben im Controller unter CODESYS V3 folgende Größen:

- Programmspeicher: 32 MByte
- Datenspeicher/Merker: 128 MByte
- Eingangsdaten: 64 kByte
- Ausgangsdaten: 64 kByte
- Retain/Persistent: 128 kByte
- Bausteinbegrenzung: 12 * 4096 Byte = 48 kByte

9.3.1 Programm- und Datenspeicher

Der Programmspeicher (auch Code-Speicher) hat eine Größe von maximal 32 MByte.
Der Datenspeicher eine Größe von maximal 128 MByte.
Beide Bereiche sind voneinander getrennt und werden abhängig vom Umfang des Programms mit dem Download im System angefordert. Eine mögliche Überschreitung der Größenbegrenzung wird dabei als Fehler angezeigt.

9.3.2 Bausteinbegrenzung

Zusammen mit dem von der Applikation nutzbaren Programm- und Datenspeicher wird für die einzelnen Programmbausteine im System Speicher zur Verwaltung benötigt.

Die Größe dieses Verwaltungsbereiches berechnet sich aus Bausteinbegrenzung * 12 (also 4096 Byte * 12).

Die Summe aus globalen Programm- und Datenspeicher und Bausteinbegrenzungsspeicher ergibt die tatsächliche Größe des im System für Daten angeforderten Arbeitsspeichers.

9.3.3 Remanenter Arbeitsspeicher

Insgesamt stehen der IEC-61131-Anwendung 128 kByte remanenten Speichers zur Verfügung.
Der remanente Bereich wird unterteilt in den Retainbereich und den Persistenzbereich. Die Bereiche werden von CODESYS V3 automatisch verteilt.

9.3.4 Dateizugriff aus der IEC-Applikation

Der Zugriff auf Dateien über die IEC-Applikation ist auf die folgenden Verzeichnisse beschränkt:

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

9.3.5 Netzwerkeinstellungen durch die IEC-Applikation ändern

Damit Netzwerkeinstellungen aus einer IEC-Anwendung heraus oder über einen Feldbus (z. B. PROFINET DCP) geändert werden können, muss der Parameter „IP Source“ auf “external” gesetzt werden (WBM-Seite „TCP/IP Configuration“ – Gruppe „Bridge Interfaces“).

Das Ändern der Netzwerkeinstellungen durch die IEC-Applikation erfolgt z. B. durch Aktivieren der Option „Einstellungen des Betriebssystems anpassen” in CODESYS (Doppelklick auf Element „Ethernet (Ethernet)“ im Gerätebaum > Register „Allgemein“ > Option „Einstellungen des Betriebssystems anpassen”).

9.3.6 EtherCAT

Die EtherCAT-Anbindung ist über die CODESYS V3-Funktionalität und die CODESYS V3-Bibliotheken möglich.

Um die EtherCAT-Master-Funktion zu nutzen, müssen die Netzwerkschnittstellen von „switched” auf „separated” umgeschaltet (WBM-Seite „Ethernet Configuration“ – Gruppe „Bridge Configuration“) und die Steuerung oder zumindest die Runtime neu gestartet werden, damit die Zuordnung der MAC-Adressen korrekt erfolgt.
Für die Konfiguration des im Projekt hinzugefügten EtherCAT-Masters wird der gewünschte Netzadapter in CODESYS ausgewählt (Doppelklick auf Element „EtherCAT_Master“ im Gerätebaum > Register „Allgemein“ > „Quelladresse MAC“ > Schaltfläche [Auswählen…]).

10 Diagnose

Zur Diagnose werten Sie die Anzeige der Status-LED auf der Frontseite aus und lesen Sie die Fehlermeldungen im WBM unter „Diagnostic“.
Die Bedeutung der möglichen Anzeigen ist wie folgt:

Tabelle 30: LED-Signalisierung

LED-Anzeige	Bedeutung
Grün leuchtend	Der Controller ist betriebsbereit.
Rot blinkend	Ein Fehler liegt vor. Die betreffende Fehlermeldung wird angezeigt.
Blau blinkend	Ein Verbindungsfehler zum Controller liegt vor; keine Kommunikation

Im Falle eines Verbindungsfehlers prüfen Sie,

- ob der Controller in Betrieb ist,
- ob die Netzwerkeinstellungen korrekt sind,
- ob die URL des Controllers korrekt ist.

Lassen sich die Fehler nicht beseitigen, kontaktieren Sie bitte den WAGO-Support. support@wago.com
Teilen Sie die Farbe mit, die ausgegeben wird.

Logbuch

Im Logbuch werden Systemmeldungen wie zum Beispiel „Start des Controllers“ oder auch „Kommunikationsabbrüche“ protokolliert.
Im Register „Diagnostic“ im WBM ist es möglich, das Logbuch auszulesen.

11 Service

11.1 Konfiguration mit dem WBM ändern

Oben befindet sich der **Taster „CFG/RST“**. Mit diesem wird das Web-Based-Management WBM zur Konfiguration des Gerätes aufgerufen. Der Taster darf nur mit einem spitzen nicht-metallischen Gegenstand gedrückt werden. Während der Laufzeit der Visualisierung wird dadurch das WBM aufgerufen. Während des Startens (Power ON) des Gerätes wird die Autostartliste unterbunden und das Gerät startet nur das WBM. Es werden keine Änderungen an den Einstellungen durch den Taster vorgenommen.

11.2 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!

Hinweis

Zur Firmware-Zielversion 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.

Verwenden Sie daher nach einer Firmwareänderung nur die zur Ziel-Firmware passende Dokumentation.

Bei Rückfragen wenden Sie sich an den WAGO Support.

Sie können die Firmware auf zwei verschiedene Arten aktualisieren:

- mit WAGOupload
- mit Speicherkarte und WBM

11.2.1 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.

11.2.2 Firmware-Update/-Downgrade mit Speicherkarte und WBM durchführen

Wenn Sie den Controller auf eine höhere Firmware-Version „updaten“ oder auf eine niedrigere Firmware-Version „downgraden“ möchten, gehen Sie folgendermaßen vor:

1. Kopieren Sie zunächst das Firmware-Image der benötigten Firmware (*.img-Datei) 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 neuen Firmware-Image in den Speicherkartensteckplatz. Verwenden Sie ggf. ein spezielles Downgrade-Image (siehe oben).

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 neuen Firmware-Version gestartet.

12 Demontieren

12.1 Demontage von der Tragschiene

11. Zur Demontage ziehen Sie die Lasche nach unten. Benutzen Sie dafür einen Schraubendreher oder ein Betätigungswerkzeug.

2. Lösen Sie das Produkt in einer Schwenkbewegung von der Tragschiene.

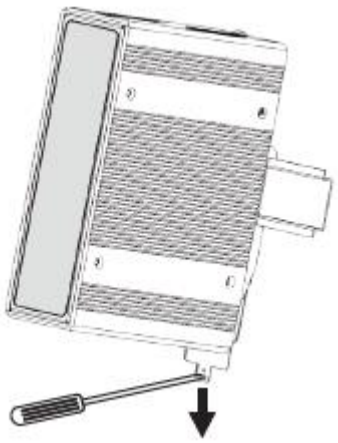

Abbildung 21: Demontage von der Tragschiene

13 Entsorgen

13.1 Elektro- und Elektronikgeräte

Elektro- und Elektronikgeräte dürfen nicht über den Hausmüll entsorgt werden. Dies gilt auch für Produkte ohne dieses Zeichen.

Elektro- und Elektronikgeräte enthalten Materialien, Stoffe und Substanzen, die umwelt- und gesundheitsschädlich sein können. Elektro- und Elektronikgeräte müssen nach Nutzungsbeendigung ordnungsgemäß entsorgt werden. Europaweit gilt die WEEE 2012/19/EU. National können abweichende Richtlinien und Gesetze gelten.

Eine umweltverträgliche Entsorgung dient der Gesundheit und schützt die Umwelt vor schädlichen Substanzen aus Elektro- und Elektronikgeräten.

- Beachten Sie die nationalen und örtlichen Vorschriften für die Entsorgung von Elektro- und Elektronikgeräten.
- Löschen Sie im Elektro- und Elektronikgerät eventuell gespeicherte Daten.
- Entnehmen Sie im Elektro- und Elektronikgerät eventuell hinzugefügte Batterie, Akku oder Speicherkarte.
- Lassen Sie die Elektro- und Elektronikgeräte ihrer örtlichen Sammelstelle zukommen.

Eine unsachgemäße Entsorgung von Elektro- und Elektronikgeräten kann umwelt- und gesundheitsschädlich sein.

13.2 Verpackung

Verpackungen enthalten Materialien, welche wiederverwendet werden können. Europaweit gelten die Verpackungsrichtlinien PPWD 94/62/EU und 2004/12/EU. National können abweichende Richtlinien und Gesetze gelten.

Eine umweltverträgliche Entsorgung der Verpackung schützt die Umwelt und ermöglicht einen nachhaltigen und effizienten Umgang mit Ressourcen.

- Beachten Sie die nationalen und örtlichen Vorschriften für die Entsorgung von Verpackungen.
- Entsorgen Sie Verpackungen aller Art so, dass ein hohes Maß an Rückgewinnung, Wiederverwendung und Recycling möglich ist.

Eine unsachgemäße Entsorgung von Verpackungen kann umweltschädlich sein und verschwendet wertvolle Ressourcen.

14 Zubehör

Für das Produkt ist eine Reihe von zertifizierten Zubehörartikeln lieferbar.

Tabelle 31: Zubehör – Speicherkarten

microSD-Speicherkarte, 1 Gbyte	758-879/000-002
microSD-Speicherkarte, 2 Gbyte	758-879/000-3102

Tabelle 32: Zubehör – Anschlussleitung und Stecker

USB-A-B-Anschlussleitung, 3 m	758-879/000-101
Federleiste (Stecker) zum Anschließen der Versorgungsspannung	734-103
Feldbusstecker CANopen	750-963

15 Anhang

15.1 Konfigurationsdialoge

15.1.1 Web-Based-Management (WBM)

15.1.1.1 Registerkarte „Information“

15.1.1.1.1 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 Angaben zur Produktidentifikation angezeigt.

Tabelle 33: 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 34: WBM-Seite „Device Status“ – Gruppe „Network TCP/IP Details“

Parameter	Bedeutung	
Bridge <n>	Aktuell konfigurierte Bridge; für jede konfigurierte Bridge 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 **Configuration** auf der Seite **Networking** > **TCP/IP Configuration** eine Bezugsquelle aus.
	static IP	Statische IP-Adressvergabe
	dhcp	Dynamische IP-Adressvergabe über DHCP
	bootp	Dynamische IP-Adressvergabe über BootP (Wenn BootP unterstützt wird.)
	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	

15.1.1.1.2 Seite „Vendor Information“

Auf der Seite „Vendor Information“ finden Sie Hersteller und Anschrift.

15.1.1.1.3 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 35: WBM-Seite „PLC Runtime Information” – Gruppe „Runtime“

Parameter	Bedeutung
Version	Hier wird die Version des aktivierten Laufzeitsystems angezeigt. Bei ausgeschaltetem Laufzeitsystem wird „None“ angezeigt.

Gruppe „WebVisu“

Hier finden Sie einen Link über den Sie die WebVisu öffnen können.

15.1.1.1.4 Seite „WAGO Software License Agreement“

Auf der Seite „WAGO Software License Agreement“ werden die Lizenzbedingungen für die im Produkt eingesetzte Software von WAGO aufgelistet.

15.1.1.1.5 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.

15.1.1.1.6 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.

15.1.1.1.7 Seite „Trademarks Information“

Auf der Seite „Trademarks Information“ finden Sie eine Auflistung der Schutz- und Markenrechte.

15.1.1.1.8 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.

15.1.1.2 Registerkarte „Configuration“

15.1.1.2.1 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“

Tabelle 36: WBM-Seite „PLC Runtime Configuration” – Gruppe „General PLC Runtime Configuration“

Parameter	Bedeutung	
PLC runtime version	Hier wählen Sie aus, welches SPS-Laufzeitsystem aktiviert ist.	
	none	Kein Laufzeitsystem ist aktiviert.
	CODESYS V3	Laufzeitsystem CODESYS V3 ist aktiviert.
Home directory on memory card enabled	Hier stellen Sie ein, ob das Home-Verzeichnis für das Laufzeitsystem auf die Speicherkarte ausgelagert werden soll.	
	Disabled	Das Home-Verzeichnis wird im internen Speicher abgelegt.
	Enabled	Das Home-Verzeichnis wird auf die Speicherkarte ausgelagert.

Hinweis

Löschen aller Daten bei Umschaltung des Laufzeitsystems!
Bei der Umschaltung des Laufzeitsystems wird das Home-Verzeichnis für das Laufzeitsystem komplett gelöscht.

Hinweis

Nur erste Partition als Home-Verzeichnis nutzbar!
Nur die erste Partition einer Speicherkarte ist unter /media/sd erreichbar und kann als Home-Verzeichnis benutzt werden.

Um die Änderung zu übernehmen, klicken Sie auf die entsprechende Schaltfläche **[Submit]**. 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!

Gruppe „Webserver Configuration“

Tabelle 37: WBM-Seite „PLC Runtime Configuration” – Gruppe „Webserver Configuration“

Parameter	Bedeutung	
CODESYS 3 Webserver State	Hier wird der Status (enabled/disabled) des CODESYS V3-Webservers angezeigt.	
Default Webserver	Hier wählen Sie aus, ob bei alleiniger Eingabe der IP-Adresse des Controllers das Web-Based-Management oder die Webvisualisierung des Laufzeitsystems angezeigt werden soll.	
	Web-based-Management	Das Web-Based-Management wird angezeigt.
	WebVisu	Die Webvisualisierung des Laufzeitsystems wird angezeigt.

Um die Änderung zu übernehmen, klicken Sie auf die Schaltfläche **[Submit]**. Die Änderung wird sofort wirksam.

Im Auslieferzustand 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-Webservers kann jederzeit das WBM mit „https://<IP-Adresse>/wbm“ und die Webvisualisierung mit „https://<IP-Adresse>/webvisu“ aufgerufen werden.

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.

15.1.1.2.2 Seite „TCP/IP Configuration“

Auf der Seite „TCP/IP Configuration“ finden Sie die TCP/IP-Einstellungen zu den ETHERNET-Schnittstellen.

Gruppe „TCP/IP Configuration“

Für jede konfigurierte Bridge werden die Eigenschaften in einem separaten Bereich dargestellt.

Tabelle 38: WBM-Seite „TCP/IP Configuration“ – Gruppe „TCP/IP Configuration“

Parameter	Bedeutung	
Network Details Bridge <n>	Einstellungen für die aktuell konfigurierte Bridge	
Current IP Address	Hier wird die aktuelle IP-Adresse angezeigt.	
Current Subnet Mask	Hier wird die aktuelle Subnetzmaske angezeigt.	
Current Default Gateway	Hier wird die IP-Adresse des aktuellen Default-Gateways angezeigt.	
IP Source	Hier wählen Sie aus, ob Sie eine statische oder dynamische IP-Adressierung verwenden möchten.	
	Static IP	Statische IP-Adressierung
	DHCP	Dynamische IP-Adressierung über DHCP
	BootP	Dynamische IP-Adressierung 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	Hier geben Sie eine statische IP-Adresse ein. Diese ist aktiv, wenn im Auswahlfeld **IP Source** der Eintrag „Static IP“ aktiviert ist.	
Subnet Mask	Hier geben Sie die Subnetzmaske ein. Diese ist aktiv, wenn im Auswahlfeld **IP Source** der Eintrag „Static IP“ aktiviert ist.	
Default Gateway	Hier geben Sie die IP-Adresse des Default-Gateways ein.	

Um eine Änderung zu übernehmen, klicken Sie die Schaltfläche **[Submit]**. Die Änderung wird sofort wirksam.

Gruppe „DNS Server“

Tabelle 39: WBM-Seite „TCP/IP Configuration“ – Gruppe „DNS Server“

Parameter	Bedeutung
Active	Hier werden die aktiven DNS-Server angezeigt. Es können bis zu 3 aktive DNS-Server genutzt werden. Der Index spiegelt die Anfrage-Reihenfolge wider. Der erste DNS-Server, der über DHCP zugewiesen wurde, erhält die höchste Priorität.
Assigned by DHCP	Hier werden die ggf. durch DHCP (oder BootP) zugewiesenen DNS-Server angezeigt. Wenn kein DNS-Server durch DHCP (oder BootP) zugewiesen wurde, wird „no DNS Servers assigned by DHCP“ angezeigt.
Assigned by user	Hier werden die Adressen der eingetragenen DNS-Server angezeigt. Wenn kein DNS-Server eingetragen wurde, erscheint die Anzeige „no DNS Servers configured“.
New Server IP	Hier fügen Sie weitere DNS-Serveradressen hinzu. Sie können maximal 3 Adressen eintragen. Die tatsächlich verwendeten Einträge ergeben sich durch eine abwechselnde Zusammenführung der Listen „Assigned by DHCP“ und „Assigned by user“.

Um den ausgewählten DNS-Server zu löschen, klicken Sie die Schaltfläche **[Delete]**. Die Änderung wird sofort wirksam.

Um den eingegebenen DNS-Server hinzuzufügen, klicken Sie die Schaltfläche **[Add]**. Die Änderung wird sofort wirksam.

15.1.1.2.3 Seite „Ethernet Configuration“

Auf der Seite „Ethernet Configuration“ finden Sie die Einstellungen zu ETHERNET.

Gruppe „Bridge Configuration“

Tabelle 40: WBM-Seite „Ethernet Configuration“ – Gruppe „Bridge Configuration“

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

Um die Änderung zu übernehmen, klicken Sie die Schaltfläche **[Submit]**. Die Änderung wird sofort wirksam.

Gruppe „Switch Configuration“

Diese Gruppe ist nur sichtbar, wenn die Konfiguration der Parameter unterstützt wird.

Tabelle 41: WBM-Seite „Ethernet Configuration“ – Gruppe „Switch Configuration“

Parameter	Bedeutung	
Port Mirror	Hier schalten Sie die Spiegelung des Datenverkehrs zwischen den Ports ein oder aus.	
	None	Beide ETHERNET-Ports arbeiten normal.
	X1	Der gesamte Datenverkehr zwischen X1 und dem PFC-System wird an Port X2 gespiegelt bereitgestellt.
	X2	Der gesamte Datenverkehr zwischen X2 und dem PFC-System wird an Port X1 gespiegelt bereitgestellt.
Broadcast Protection	Hier stellen Sie die Broadcast-Begrenzung zum Schutz vor Überlastung ein.	
	Disabled	Keine Begrenzung von Broadcast-Paketen
	1 % … 5 %	Limitierung der eingehenden Broadcast-Pakete auf den ausgewählten Prozentsatz vom insgesamt möglichen Datendurchsatz (10/100Mbit)
Rate Limit	Hier stellen Sie die grundsätzliche Begrenzung des eingehenden Datenverkehrs ein.	
	Disabled	Keine Limitierung des eingehenden Datenverkehrs
	64 kbps … 99 mbps	Limitierung des eingehenden Datenverkehrs auf den angegebenen Wert

Um die Änderung zu übernehmen, klicken Sie die entsprechende Schaltfläche **[Submit]**. Die Änderung wird sofort wirksam.

Gruppe „Dummy Interfaces“

Tabelle 42: WBM-Seite „Ethernet Configuration“ – Gruppe „Dummy Interfaces“

Parameter	Bedeutung
Name	Name des ausgewählten Dummy-Interfaces
Add Dummy Interface	Neues Dummy-Interface anlegen
Name	Namen des neuen Dummy-Interfaces eingeben

Um einen ausgewählten Eintrag zu löschen, klicken Sie auf die Schaltfläche **[Delete]**. Die Änderungen werden sofort wirksam.

Um einen neuen Eintrag anzulegen, klicken Sie auf die Schaltfläche **[Add]**. Die Änderungen werden sofort wirksam.

Gruppe „VLAN Interfaces“

Tabelle 43: 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
Add	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

Um einen ausgewählten Eintrag zu löschen, klicken Sie auf die Schaltfläche **[Delete]**. Die Änderungen werden sofort wirksam.

Um einen neuen Eintrag anzulegen, klicken Sie auf die Schaltfläche **[Add]**. Die Änderungen werden sofort wirksam.

Gruppe „Ethernet Interface Configuration“

Tabelle 44: WBM-Seite „Ethernet Configuration“ – Gruppe „Ethernet Interface Configuration“

Parameter	Bedeutung
Interface X<n>	Für jedes im Controller vorhandene Interface wird ein eigener Bereich angezeigt.
Enabled	Hier können Sie das Interface aktivieren bzw. deaktivieren.
MAC Learning	Hier können Sie „MAC Learning“ deaktivieren bzw. aktivieren.
Speed/Duplex	Hier wählen Sie die Übertragungsgeschwindigkeit und das Übertragungsverfahren aus. Die Auswahlliste wird geräte- und interface-abhängig generiert. Mit der Auswahl „Autonegotiation“ werden die Verbindungsmodalitäten automatisch mit der Gegenstelle ausgehandelt.

Um die Änderungen zu übernehmen, klicken Sie auf die Schaltfläche **[Submit]**.
Die Änderungen werden sofort wirksam.

15.1.1.2.4 Seite „Configuration of Host and Domain Name“

Auf der Seite „Configuration of Host and Domain Name“ finden Sie die Einstellungen zum Hostnamen und zum Domain-Namen.

Gruppe „Hostname“

Tabelle 45: WBM-Seite „Configuration of Host and Domain Name“ – Gruppe „Hostname“

Parameter	Bedeutung
Currently used	Wenn Sie die dynamische Zuweisung einer IP-Adresse über DHCP ausgewählt haben, wird hier der Name des aktuell verwendeten Hosts angezeigt.
Configured	Hier geben Sie den Hostnamen Ihres Produkts ein, der dann verwendet werden soll, wenn die Netzwerk-Schnittstelle auf eine statische IP-Adresse geändert wird oder wenn per DHCP-Antwort kein Hostname übertragen wird.

Um eine Änderung zu übernehmen, klicken Sie die Schaltfläche **[Submit]**.

Um ein Eingabefeld zurückzusetzen, klicken Sie die Schaltfläche **[Clear]**.

Die Änderung wird sofort wirksam.

Wenn der Controller per DHCP einen Hostnamen zugewiesen bekommen hat, wird dieser bevorzugt eingestellt und der manuell konfigurierte wird nicht verwendet.
Um den manuell konfigurierten Hostnamen zu übernehmen, muss ggf. die Konfiguration des DHCP-Servers um die Zuweisung des Hostnamens reduziert werden.

Gruppe „Domain Name“

Tabelle 46: WBM-Seite „Configuration of Host and Domain Name“ – Gruppe „Domain Name“

Parameter	Bedeutung
Currently used	Wenn Sie die dynamische Zuweisung einer IP-Adresse über DHCP ausgewählt haben, wird hier der Name der aktuell verwendeten Domain angezeigt.
Configured	Hier geben Sie den Domain-Namen Ihres Produkts ein, der dann verwendet werden soll, wenn die Netzwerk-Schnittstelle auf eine statische IP-Adresse geändert wird oder wenn per DHCP-Antwort kein Domain-Name übertragen wird.

Um eine Änderung zu übernehmen, klicken Sie die Schaltfläche **[Submit]**.

Um ein Eingabefeld zurückzusetzen, klicken Sie die Schaltfläche **[Clear]**.

Die Änderung wird sofort wirksam.

Wenn der Controller per DHCP einen Domainnamen zugewiesen bekommen hat, wird dieser bevorzugt eingestellt und der manuell konfigurierte wird nicht verwendet.
Um den manuell konfigurierten Domainnamen zu übernehmen, muss ggf. die Konfiguration des DHCP-Servers um die Zuweisung des Domainnamens reduziert werden.

15.1.1.2.5 Seite „Routing“

Auf der Seite „Routing“ finden Sie Einstellungen und Informationen zum Routing zwischen den Netzwerkschnittstellen.

Gruppe „IP Forwarding through multiple interfaces“

Tabelle 47: WBM-Seite „Routing“ – Gruppe „IP Forwarding through multiple interfaces“

Parameter	Bedeutung
Enabled	Hier stellen Sie ein, ob die Weiterleitung von IP-Datenpaketen zwischen unterschiedlichen Netzwerkschnittstellen erlaubt ist. Ist das Kontrollfeld nicht markiert, werden die Einstellungen unter „Static Routes“ angewendet, ohne dass IP-Datenpakete, die die Steuerung auf einer Netzwerkschnittstelle erreichen, die Steuerung auf einer anderen Netzwerkschnittstelle verlassen dürfen. Ist das Kontrollfeld markiert, können IP-Pakete zwischen den Interfaces weitergeleitet werden. Ggf. sind weitere Einstellungen auf dieser WBM-Seite erforderlich.

Um die Änderung zu übernehmen, klicken Sie die Schaltfläche **[Submit]**. Die Änderungen werden 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 48: WBM-Seite „Routing“ – Gruppe „Custom Routes“

Parameter	Bedeutung	
Enabled	Hier stellen Sie ein, ob die ausgewählte Route verwendet werden soll.	
	Disabled	Die Route wird nicht verwendet.
	Enabled	Die Route wird verwendet.
Destination Address	Hier geben Sie ein, ob beliebige oder nur ein bestimmter Netzwerkteilnehmer oder ein Teilnehmer-Pool erreichbar sein soll.	
	default	Es sind beliebige Netzwerkteilnehmer erreichbar.
	Netzwerkadresse	Es ist nur ein bestimmter Teilnehmer oder Teilnehmer aus dem vorgegebenen Adress-Pool erreichbar.
Destination Mask	Hier geben Sie die Subnet-Maske des Teilnehmers ein. Wenn bei Destination-Address „default“ eingetragen ist, muss hier der Wert „0.0.0.0“ eingetragen werden.	
Gateway Address	Hier stellen Sie die Adresse des Gateways ein. Ist das Eingabefeld „Interface“ leer, ist hier eine Eingabe erforderlich. Wird im Eingabefeld „Interface“ ein Wert eingetragen, ist die Eingabe hier optional.	
Gateway Metric	Hier stellen Sie die Zahl als Metrik ein. 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	Hier geben Sie ein Interface ein, 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.	

Um die Änderungen zu übernehmen, klicken Sie die Schaltfläche **[Submit]**. Die Änderungen werden sofort wirksam.

Um eine neue Route hinzuzufügen, klicken Sie die Schaltfläche **[Add]**. Die Änderung wird sofort wirksam.

Um eine bestehende Route zu löschen, klicken Sie die Schaltfläche **[Delete]**. Die Änderung wird sofort wirksam.

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 routes)“ angezeigt.

Gruppe „IP-Masquerading“

Für jeden Eintrag wird ein eigener Bereich angezeigt. Wenn keine Einträge vorhanden sind, wird „(no masquerading configured)“ angezeigt.

Tabelle 49: WBM-Seite „Routing“ – Gruppe „IP-Masquerading“

Parameter	Bedeutung	
Enabled	Hier stellen Sie ein, ob IP-Masquerading verwendet werden soll.	
	Disabled	IP-Masquerading wird nicht verwendet.
	Enabled	IP-Masquerading wird verwendet.
Interface	Hier können Sie einen der angegebenen Namen eines Netzwerk-Interfaces auswählen. Alternativ kann über die Auswahl von „other“ ein beliebiger Netzwerk-Interface-Name angegeben werden.	

Um die Änderungen zu übernehmen, klicken Sie die Schaltfläche **[Submit]**. Die Änderungen werden sofort wirksam.

Um einen neuen Eintrag hinzuzufügen, klicken Sie die Schaltfläche **[Add]**. Die Änderung wird sofort wirksam.

Um einen bestehenden Eintrag zu löschen, klicken Sie die Schaltfläche **[Delete]**. Die Änderung wird sofort wirksam.

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. Wenn keine Einträge vorhanden sind, wird „(no Port Forwarding configured)“ angezeigt.

Tabelle 50: WBM-Seite „Routing“ – Gruppe „Port-Forwarding“

Parameter	Bedeutung	
Enabled	Hier stellen Sie ein, ob Port-Forwarding verwendet werden soll.	
	Disabled	Port-Forwarding wird nicht verwendet.
	Enabled	Port-Forwarding wird verwendet.
Interface	Hier können Sie einen der angegebenen Namen eines Netzwerk-Interfaces auswählen. Alternativ kann über die Auswahl von „other“ ein beliebiger Netzwerk-Interface-Name angegeben werden.	
Port	Hier geben Sie den Port ein, auf dem weiterzuleitende Netzwerk-Datenpakete das Produkt erreichen.	
Protocol	Hier kann das Protokoll ausgewählt werden, welches für das Port-Forwarding berücksichtigt werden soll. Zur Auswahl stehen TCP, UDP oder beide Protokolle.	
Destination Address	Hier stellen Sie die Netzwerkadresse des Zielteilnehmers ein. Diese Adresse ersetzt die ursprüngliche Destination-Address des Netzwerk-Datenpakets.	
Destination Port	Hier stellen Sie die Port-Nummer des Zielteilnehmers ein. Dieser Wert ersetzt den ursprünglichen Destination-Port des Netzwerk-Datenpakets.	

Um die Änderungen zu übernehmen, klicken Sie die Schaltfläche **[Submit]**. Die Änderungen werden sofort wirksam.

Um einen neuen Eintrag hinzuzufügen, klicken Sie die Schaltfläche **[Add]**. Die Änderung wird sofort wirksam.

Um einen bestehenden Eintrag zu löschen, klicken Sie die Schaltfläche **[Delete]**. Die Änderung wird sofort wirksam.

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.

15.1.1.2.6 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 51: WBM-Seite „Spanning Tree Protocol“– Gruppe „Status“

Parameter	Bedeutung	
Current Status	Hier wird der aktuelle Status angezeigt.	
	Deaktiviert	STP/RSTP ist nicht aktiv.
	Aktiviert	STP/RSTP ist aktiv.
Current Bridge	Hier wird die ausgewählte Bridge angezeigt.	
Current Mode	Hier wird das aktuelle Protokoll angezeigt.	
	STP	Spanning Tree Protocol ist aktiv.
	RSTP	Rapid Spanning Tree Protocol ist aktiv.
Current Priority	Hier wird die aktuelle Bridge-Priorität angezeigt.	
Current Hello Time (sec)	Hier wird die aktuelle „Hello“-Zeit in Sekunden angezeigt.	
Current Forward Delay (sec)	Hier wird die aktuelle „Forward Delay“-Zeit in Sekunden angezeigt.	
Current Max Age (sec)	Hier wird die aktuelle „Max Age“-Zeit in Sekunden angezeigt.	
Current Max Hops	Hier wird die aktuelle „Max Hops“-Anzahl angezeigt.	
Current Path Cost	Hier werden die aktuellen „Path Cost“ angezeigt.	
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	Hier wird der aktuelle „Bpdu Filter“-Status angezeigt.	
	Deaktiviert	Bpdu-Filter ist nicht aktiv.
	Aktiviert	Bpdu-Filter ist aktiv.
Current Bpdu Guard	Hier wird der aktuelle „Bpdu Guard“-Status angezeigt.	
	Deaktiviert	Bpdu-Guard ist nicht aktiv.
	Aktiviert	Bpdu-Guard ist aktiv.
Current Edge Port	Hier wird der aktuelle Port-Status angezeigt.	
	Deaktiviert	Port ist kein Edge-Port.
	Aktiviert	Port ist Edge-Port.
Current Root Guard	Hier wird der aktuelle „Root Guard“-Status angezeigt.	
	Deaktiviert	Root-Guard ist nicht aktiv.
	Aktiviert	Root-Guard ist aktiv.
Current Path Cost	Hier werden die aktuellen „Path Cost“ angezeigt.	

Tabelle 51: WBM-Seite „Spanning Tree Protocol“– Gruppe „Status“

Parameter	Bedeutung	
Current Priority	Hier wird die aktuelle Priorität angezeigt.	
Current Role	Hier wird die aktuelle Rolle des Ports angezeigt.	
	Disabled	Der Port ist deaktiviert.
	Designated	Der in jedem LAN-Segment ausgewählte Port, der die niedrigsten Root-Pfadkosten bietet. Je höher die Verbindungsgeschwindigkeit, desto niedriger ist der Kostenwert.
Current Status	Hier wird der aktuelle Status des Ports angezeigt.	
	Discarding	Der Port kann Daten senden und empfangen, MACAdressen lernen und Daten an ihr Ziel weiterleiten.
	Forwarding	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 52: WBM-Seite „Spanning Tree Protocol“– Gruppe „Parameter Settings“

Parameter	Bedeutung	
Enabled	Hier aktivieren/deaktivieren Sie das Spanning Tree Protocol.	
	Deaktiviert	Spanning Tree Protocol ist nicht aktiv.
	Aktiviert	Spanning Tree Protocol ist aktiv.
Bridge	Hier wählen Sie die Bridge aus.	
Mode	Hier wählen Sie das Protokoll aus.	
	STP	Spanning Tree Protocol
	RSTP	Rapid Spanning Tree Protocol
Priority	Hier stellen Sie die Bridge-Priorität ein; Zulässige Werte: 1 … 15	
Hello Time	Hier stellen Sie die „Hello“-Zeit in Sekunden ein; Zulässige Werte: 1 … 19	
Forward Delay	Hier stellen Sie die „Forward Delay“-Zeit in Sekunden ein; Zulässige Werte: 4 … 30	
Max Age	Hier stellen Sie die „Max Age“-Zeit in Sekunden ein; Zulässige Werte: 6 … 40	
Max Hops	Hier stellen Sie die „Max Hops“-Anzahl ein; Zulässige Werte: 6 … 40	
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.	
Current Bpdu Filter	Hier aktivieren/deaktivieren Sie den „Bpdu Filter“.	
	Deaktiviert	Bpdu-Filter ist nicht aktiv.
	Aktiviert	Bpdu-Filter ist aktiv.
Current Bpdu Guard	Hier aktivieren/deaktivieren Sie den „Bpdu Guard“.	
	Deaktiviert	Bpdu-Guard ist nicht aktiv.
	Aktiviert	Bpdu-Guard ist aktiv.
Current Edge Port	Hier aktivieren/deaktivieren Sie den Port als Edge-Port.	
	Deaktiviert	Port ist kein Edge-Port.
	Aktiviert	Port ist Edge-Port.
Current Root Guard	Hier aktivieren/deaktivieren Sie den „Root Guard“.	
	Deaktiviert	Root-Guard ist nicht aktiv.
	Aktiviert	Root-Guard ist aktiv.
Current Path Cost	Hier stellen Sie die „Path Cost“ ein; Zulässige Werte: 0 … 65535	

Tabelle 52: WBM-Seite „Spanning Tree Protocol“– Gruppe „Parameter Settings“

Parameter	Bedeutung
Current Priority	Hier stellen Sie die Priorität ein; Zulässige Werte: 0 …15, Default = 8

Um die Änderungen zu übernehmen, klicken Sie die Schaltfläche **[Submit]**. Die Änderungen werden sofort wirksam.

15.1.1.2.7 Seite „Clock Settings“

Auf der Seite „Clock Settings“ finden Sie die Einstellungen zu Datum und Uhrzeit.

Gruppe „Timezone and Format“

Tabelle 53: WBM-Seite „Clock Settings“ – Gruppe „Timezone and Format“

Parameter	Bedeutung	
Timezone	Hier wählen Sie die für Ihr Land zutreffende Zeitzone aus. 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	Für nicht über den Parameter „Time Zone“ auswählbare Zeitzonen geben Sie hier den Namen der für Sie zutreffenden Zeitzone oder das zutreffende Land und die zutreffende Stadt ein. Einen gültigen Namen für die Zeitzone können Sie hier ermitteln: http://www.timeanddate.com/time/map/	
Time Format	Umschaltung zwischen 12h- und 24h-Darstellung der Uhrzeit	

Um eine Änderung zu übernehmen, klicken Sie die Schaltfläche **[Submit]**. Die Änderung wird sofort wirksam.

Gruppe „UTC Time and Date“

Tabelle 54: WBM-Seite „Clock Settings“ – Gruppe „UTC Time and Date“

Parameter	Bedeutung
UTC Date	Hier stellen Sie das Datum ein.
UTC Time	Hier stellen Sie die GMT-Zeit ein.

Um eine Änderung zu übernehmen, klicken Sie die Schaltfläche **[Submit]**. Die Änderung wird sofort wirksam.

Gruppe „Local Time and Date“

Tabelle 55: WBM-Seite „Clock Settings“ – Gruppe „Local Time and Date“

Parameter	Bedeutung
Local Date	Hier stellen Sie das Datum ein.
Loacl Time	Hier stellen Sie die lokale Uhrzeit ein.

Um eine Änderung zu übernehmen, klicken Sie die Schaltfläche **[Submit]**. Die Änderung wird sofort wirksam.

15.1.1.2.8 Seite „Configuration of Serial Interface“

Auf der Seite „Configuration of Serial Interface“ finden Sie die Einstellungen zur seriellen Schnittstelle.

Gruppe „Current Serial Interface Configuration“

Tabelle 56: WBM-Seite „Configuration of Serial Interface” – Gruppe „Current Serial Interface Configuration“

Parameter	Bedeutung	
Assigned to	Hier wird die aktuelle Zuordnung der Kommunikationsschnittstelle angezeigt.	
	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	Hier wird der aktuelle Modus der Kommunikationsschnittstelle angezeigt.	
	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 serielle Schnittstelle nach dem nächsten Controller-Reboot zugewiesen wird.

Tabelle 57: WBM-Seite „Configuration of Serial Interface” – Gruppe „Assign Owner of Serial Interface“

Parameter	Bedeutung
Linux® Console	Hier wählen Sie aus, dass die serielle Schnittstelle der Linux®-Konsole zugewiesen wird.
Unassigned (usage by Applications, Libraries, CODESYS)	Hier wählen Sie aus, dass die serielle Schnittstelle keiner Applikation zugewiesen wird und frei ist, damit beispielsweise das CODESYS Programm über Funktionsbausteine darauf zugreifen kann.

Um die Änderung zu übernehmen, klicken Sie auf die Schaltfläche **[Submit]**. Die Änderung wird erst nach dem nächsten Neustart des Controllers wirksam.

Nutzen Sie hierzu die Reboot-Funktion des WBM. Schalten Sie den Controller nicht zu früh aus!

Gruppe „Assign Mode of Serial Interface“

Hier können Sie den Modus auswählen, in dem die serielle Schnittstelle nach dem nächsten Controller-Reboot betrieben wird. Eine Änderung des Modus ist nur möglich, wenn die serielle Schnittstelle auf „Unassigned“ eingestellt ist.

Tabelle 58: WBM-Seite „Configuration of Serial Interface” – Gruppe „Assign Owner of Serial Interface“

Parameter	Bedeutung
RS232	Hier wählen Sie aus, dass die serielle Schnittstelle im „RS-232“-Modus betrieben wird.
RS485	Hier wählen Sie aus, dass die serielle Schnittstelle im „RS-485“-Modus betrieben wird.

Um die Änderung zu übernehmen, klicken Sie auf die Schaltfläche **[Submit]**. Die Änderung wird erst nach dem nächsten Neustart des Controllers wirksam.
Nutzen Sie hierzu die Reboot-Funktion des WBM. Schalten Sie den Controller nicht zu früh aus!

15.1.1.2.9 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 59: WBM-Seite „Configuration of Service Interface” – Gruppe „Assign Owner of Service Interface“

Parameter	Bedeutung
WAGO Service Communication	Hier wählen Sie aus, dass die Service-Schnittstelle für die WAGO Service-Kommunikation bzw. Laufzeitsystem-Kommunikation verwendet wird.
Linux Console	Hier wählen Sie aus, dass die Service-Schnittstelle der Linux®-Konsole zugewiesen wird.
Unassigned (usage by Applications, Libraries, CODESYS)	Hier wählen Sie aus, dass die Service-Schnittstelle keiner Applikation zugewiesen wird und frei ist, damit beispielsweise das CODESYS Programm über Funktionsbausteine darauf zugreifen kann.

Um die Änderung zu übernehmen, klicken Sie auf die Schaltfläche **[Submit]**. Die Änderung wird erst nach dem nächsten Neustart des Controllers wirksam. Nutzen Sie hierzu die Reboot-Funktion des WBM. Schalten Sie den Controller nicht zu früh aus!

15.1.1.2.10 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 60: WBM-Seite „Create bootable Image” – Gruppe „Create bootable image from boot device“

Parameter	Bedeutung		
Boot Device	Hier wird das Medium angezeigt, von dem gebootet wurde.		
Destination	Abhängig von welchem Medium gebootet wurde, steht nach dem Boot-Vorgang folgendes Ziel für das zu erstellende Image zur Auswahl:		
	System wurde gebootet von		Zielpartition für „bootable Image“
	Speicherkarte	→	Internal Flash
	Interner Speicher	→	Memory Card

- Freier Speicher auf dem Ziel-Device:
  Beträgt der freie Speicher weniger als 5 %, wird eine entsprechende Warnung ausgegeben. Sie können den Kopiervorgang trotzdem starten. Ist der freie Speicher definitiv zu gering, wird eine entsprechende Meldung ausgegeben, und der Vorgang kann nicht gestartet werden.

- Device in Benutzung durch CODESYS:
  Wird das Device durch CODESYS benutzt, wird eine entsprechende Warnung ausgegeben. Sie können den Kopiervorgang trotzdem starten, davon wird jedoch abgeraten!

Um den Kopiervorgang zu starten, klicken Sie die Schaltfläche **[Start Copy]**. Bei positivem Testausgang startet der Vorgang sofort. Wurden Fehler festgestellt, wird eine entsprechende Meldung angezeigt und der Vorgang wird nicht gestartet. Falls Warnungen vorliegen, werden diese noch einmal angezeigt und Sie müssen bestätigen, dass Sie den Vorgang trotzdem fortsetzen möchten.

15.1.1.2.11 Seite „Firmware Backup“

Auf der Seite „Firmware Backup“ finden Sie die Einstellungen zur Sicherung der Controllerdaten.

Gruppe „Firmware Backup“

Tabelle 61: WBM-Seite „Firmware Backup“ – Gruppe „Firmware Backup“

Parameter	Bedeutung	
Boot Device	Hier wird das Speichermedium angezeigt, von dem das Gerät gebootet wurde.	
Destination	Hier wählen Sie das Speicherziel für das Back-up aus.	
	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.
	Network	Die Daten werden im File-System gespeichert und anschließend auf dem PC als Download zur Verfügung gestellt.
PLC Runtime Project	Wenn Sie das SPS-Laufzeit-Projekt („PLC-Runtime-Projekt“, Boot-Projekt, CODESYS Einstellungen) sichern wollen, markieren Sie dieses Kontrollfeld.	
Settings	Wenn Sie die Geräteeinstellungen sichern wollen, markieren Sie dieses Kontrollfeld.	
System	Wenn Sie das Betriebssystem des Geräts und das Root-Dateisystem sichern wollen, markieren Sie dieses Kontrollfeld.	
Encryption	Wenn Sie die Daten verschlüsselt sichern wollen, markieren Sie diese Schaltfläche.	
Encryption passphrase	Hier geben Sie das Verschlüsselungspasswort ein. Dieses Eingabefeld ist nur sichtbar, wenn das Kontrollfeld Encryption markiert ist.	
Confirm passphrase	Hier geben Sie das Verschlüsselungspasswort zur Kontrolle erneut ein. Dieses Eingabefeld ist nur sichtbar, wenn das Kontrollfeld Encryption markiert ist.	

Hinweis

Firmwareversion beachten!
Das Wiederherstellen des Controllerbetriebssystems (Auswahl „System“) ist nur zulässig und möglich, wenn die Firmwareversionen zum Sicherungs- und Wiederherstellzeitpunkt gleich sind.
Verzichten Sie ggf. auf die Wiederherstellung des Controllerbetriebssystems oder gleichen Sie vorher die Firmwareversion des Controllers 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.

Hinweis

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

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.

Um den Back-up-Vorgang zu starten, klicken Sie die Schaltfläche **[Create Backup]**.

15.1.1.2.12 Seite „Firmware Restore“

Auf der Seite „Firmware Restore“ finden Sie die Einstellungen zur Wiederherstellung der Controllerdaten.

Gruppe „Firmware Restore“

Tabelle 62: WBM-Seite „Firmware Restore“ – Gruppe „Firmware Restore“

Parameter	Bedeutung	
Source	Hier wählen Sie die Datenquelle für die Wiederherstellung aus.	
	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.
	Network	Die Daten werden vom PC hochgeladen und wiederhergestellt.
Boot Device	Hier wird das Speichermedium angezeigt, von dem das Gerät gebootet wurde.	
PLC Runtime Project	Hier geben Sie den Namen der Back-up-Datei für das CODESYS Projekt ein. Das Eingabefeld ist nur aktiv, wenn als Datenquelle das Netzwerk ausgewählt ist.	
Settings	Hier geben Sie den Namen der Back-up-Datei für die Einstellungen ein. Das Eingabefeld ist nur aktiv, wenn als Datenquelle das Netzwerk ausgewählt ist.	
System	Hier geben Sie den Namen der Back-up-Datei für die Systemdaten und das Root-Dateisystem ein. Das Eingabefeld ist nur aktiv, wenn als Datenquelle das Netzwerk ausgewählt ist.	
Decryption	Wenn Sie die Daten verschlüsselt gesichert wurden, markieren Sie dieses Kontrollfeld.	
Decryption passphrase	Hier geben Sie das Verschlüsselungspasswort ein. Dieses Eingabefeld ist nur sichtbar, wenn das Kontrollfeld Decryption markiert ist.	

Hinweis

Firmwareversion beachten!
Das Wiederherstellen des Controllerbetriebssystems (Auswahl „System“) ist nur zulässig und möglich, wenn die Firmwareversionen zum Sicherungs- und Wiederherstellzeitpunkt gleich sind.
Verzichten Sie ggf. auf die Wiederherstellung des Controllerbetriebssystems oder gleichen Sie vorher die Firmwareversion des Controllers 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 Gerät 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 Gerät aufbauen. Sie müssen das WBM neu mit der korrekten IP-Adresse des Gerätes in der Adresszeile aufrufen.

Hinweis

Restore-Zeit beachten
Der Restore-Vorgang benötigt ca. 2 … 3 Minuten.
Nach dem Restore-Vorgang wird der Controller neu gestartet und ist danach wieder einsatzbereit.

Um den Wiederherstellvorgang zu starten, klicken Sie die Schaltfläche **[Restore]**.

15.1.1.2.13 Seite „Active System“

Auf der Seite „Active System“ finden Sie die Einstellungen zur Auswahl der Partition, von der das System gestartet werden soll.

Gruppe „Boot Device“

Tabelle 63: WBM-Seite „Active System“ – Gruppe „Boot Device“

Parameter	Bedeutung
Boot Device	Hier wird das Speichermedium angezeigt, von dem das Gerät gebootet wurde.

Gruppen „System <n> (Internal Flash)“

Tabelle 64: WBM-Seite „Active System“ – Gruppe „System <n> (Internal Flash)“

Parameter	Bedeutung	
Active	Hier wird angezeigt, ob das System aktiv ist.	
Configured	Hier wird angezeigt, ob das System nach dem nächsten Reboot-Vorgang aktiv sein soll.	
State	Hier wird der Status des Systems angezeigt.	
	good	Das System ist gültig und kann verwendet werden.
	bad	Das System ist nicht gültig und kann nicht verwendet werden.

Um beim nächsten Reboot-Vorgang das gewünschte System zu starten, klicken Sie die entsprechende Schaltfläche **[Activate]**.

Hinweis

Boot-fähiges System bereitstellen!
Auf dem Boot-System muss ein funktionsfähiges Firmware-Backup vorhanden sein!

15.1.1.2.14 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 65: WBM-Seite „Mass Storage“ – Gruppe „Devices“

Parameter	Bedeutung
<Device>	Hier wird das Speichermedium angezeigt.
Boot device	Hier wird angezeigt, ob von diesem Speichermedium gebootet wurde.
Volume name	Hier wird der Name des Speichermediums angezeigt.

Gruppe „Create new Filesystem on Memory Card“

Tabelle 66: WBM-Seite „Mass Storage“ – Gruppe „Create new Filesystem on Memory Card“

Parameter	Bedeutung	
Filesystem type	Hier wählen Sie das Format aus, mit dem das Dateisystem auf der Speicherkarte neu erstellt wird.	
	Ext4	Das Dateisystem wird im Ext4-Format erstellt. Die Dateien sind unter Windows nicht lesbar!
	FAT	Das Dateisystem wird im FAT-Format erstellt.
Label	Geben Sie hier den Namen ein, den das Speichermedium beim Formatieren erhalten soll.	

Hinweis

Daten werden gelöscht!
Mit dem Formatieren werden die auf dem Speichermedium gespeicherten Daten gelöscht!

Um das angegebene Speichermedium zu formatieren, klicken Sie auf **[Start]**.

15.1.1.2.15 Seite „Software Uploads“

Auf der Seite „Software Uploads“ können Softwarepakete von Ihrem PC auf das Produkt installiert werden.

Hinweis

IPKs nur aus vertrauenswürdigen Quellen installieren!
IPKs werden mit erweiterten Rechten (root-Rechte) installiert, solange es in den Metadaten nicht anders angegeben ist.
Bitte seien Sie vorsichtig bei der Installation von IPKs und installieren Sie diese nur aus vertrauenswürdigen Quellen.

Tabelle 67: WBM-Seite „Software Uploads“ – Gruppe „Upload new Software“

Parameter	Bedeutung
Software file	Hier erscheint der Dateiname Ihres ausgewählten Softwarepaketes, solange Sie es noch nicht auf das Produkt übertragen haben. Haben Sie noch kein Paket ausgewählt, erscheint der Text „Choose ipk file ...“. Klicken Sie auf das Eingabefeld und wählen Sie eine Datei mit einem Softwarepaket auf Ihrem PC aus.

Um das Paket zu installieren, klicken Sie **[Install]**.

Nach dem Installationsvorgang wird die Datei mit dem Softwarepaket wieder vom Gerät gelöscht. Sollte dies durch Fehler bei der Verarbeitung nicht möglich sein, erfolgt das Löschen spätestens beim nächsten Neustart des Produktes.

15.1.1.2.16 Seite „Configuration of Network Services“

Auf der Seite „Configuration of Network Services“ finden Sie die Einstellungen zu verschiedenen Diensten.

Hinweis

Nicht benötigte Ports und Dienste schließen!
Durch geöffnete Ports können Unbefugte Zugriff auf Ihr Automatisierungssystem erhalten.
Um die Gefahr von Cyber-Angriffen 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).
Öffnen Sie die Ports und Dienste nur für die Dauer der Inbetriebnahme bzw. Konfiguration.

Gruppe „FTP“

Tabelle 68: WBM-Seite „Configuration of Network Services“ – Gruppe „FTP“

Parameter	Bedeutung
Service active	Hier aktivieren/deaktivieren Sie den FTP-Service. In der Werkseinstellung ist dieser Service nicht aktiviert.

Um eine Änderung zu übernehmen, klicken Sie die Schaltfläche **[Submit]**. Die Änderung wird sofort wirksam.

Gruppe „FTPES (explicit FTPS)“

Tabelle 69: WBM-Seite „Configuration of Network Services“ – Gruppe „FTPES (explicit FTPS)“

Parameter	Bedeutung
Service active	Hier aktivieren/deaktivieren Sie den FTPS-Service. In der Werkseinstellung ist dieser Service nicht aktiviert.

Um eine Änderung zu übernehmen, klicken Sie die Schaltfläche **[Submit]**. Die Änderung wird sofort wirksam.

Gruppe „HTTP“

Tabelle 70: WBM-Seite „Configuration of Network Services“ – Gruppe „HTTP“

Parameter	Bedeutung
Service active	Hier aktivieren/deaktivieren Sie den HTTP-Service. In der Werkseinstellung ist dieser Service nicht aktiviert.

Um eine Änderung zu übernehmen, klicken Sie die Schaltfläche **[Submit]**. Die Änderung wird sofort wirksam.

Hinweis

Verbindungsabbruch bei Deaktivierung
Wenn der HTTP-Service deaktiviert wird, kann die Verbindung zum Produkt unterbrochen werden. Rufen Sie dann die Seite erneut auf.

Gruppe „HTTPS“

Tabelle 71: WBM-Seite „Configuration of Network Services“ – Gruppe „HTTPS“

Parameter	Bedeutung
Service active	Hier wird der Status des HTTPS-Service angezeigt.

Gruppe „I/O-*CHECK*“

Diese Gruppe ist nur sichtbar, wenn der Controller WAGO-I/O-*CHECK* unterstützt.

Tabelle 72: WBM-Seite „Configuration of Network Services“ – Gruppe „I/O-*CHECK*“

Parameter	Bedeutung
Service active	Hier aktivieren/deaktivieren Sie den WAGO-I/O-*CHECK*-Service.

Um eine Änderung zu übernehmen, klicken Sie die Schaltfläche **[Submit]**. Die Änderung wird sofort wirksam.

15.1.1.2.17 Seite „Configuration of NTP Client“

Auf der Seite „Configuration of NTP Client“ finden Sie die Einstellungen zum NTP-Dienst.

Gruppe „NTP Client Configuration“

Tabelle 73: WBM-Seite „Configuration of NTP Client“ – Gruppe „NTP Client Configuration“

Parameter	Bedeutung
Service enabled	Hier aktivieren/deaktivieren Sie die Aktualisierung der Uhrzeit.
Update Interval (sec)	Hier legen Sie das Aktualisierungsintervall des Time-Servers fest.
Time Server <n>	Hier geben Sie die IP-Adressen von maximal 4 Time-Servern ein. Time-Server Nr. 1 wird als erstes angefragt. Sind über diesen keine Daten erreichbar, wird Time-Server Nr. 2 angefragt usw.
Additionally assigned (DHCP)	Hier werden die ggf. durch DHCP (oder BootP) zugewiesenen NTP-Server angezeigt. Wenn kein NTP-Server durch DHCP (oder BootP) zugewiesenen wurde, wird „(no additional servers assigned)“ angezeigt.

Um die Zeit unabhängig vom Intervall zu aktualisieren, klicken Sie die Schaltfläche **[Update Time]**.

Um die Änderungen zu übernehmen, klicken Sie die Schaltfläche **[Submit]**. Die Änderungen werden sofort wirksam.

15.1.1.2.18 Seite „PLC Runtime Services“

Auf der Seite „PLC Runtime Services“ finden Sie die Einstellungen zu verschiedenen Diensten des Laufzeitsystems.

Gruppe „CODESYS V3“

Tabelle 74: WBM-Seite „PLC Runtime Services“ – Gruppe „CODESYS V3“

Parameter	Bedeutung
CODESYS V3 State	Hier wird der Status des CODESYS V3-Laufzeitsystems angezeigt (enabled/disabled).
Webserver enabled	Hier aktivieren oder deaktivieren Sie den Webserver für die CODESYS V3-Webvisualisierung.
Seperated WebVisu ports (8080/8081)	Hier gebe Sie an, ob die CODESYS V3-Webvisualisierung auf den Ports 8080/8081 bereitgestellt wird. In der Default-Einstellung wird die Webvisualisierung auf den WBM-Ports 80/443 bereitgestellt.
Port authentication enabled	Hier geben Sie an, ob für die Verbindung zum Gerät ein Log-in erforderlich ist. Der Benutzername ist admin und das Passwort ist das unter „General Configuration“ angegebene Passwort.

Um die Änderung zu übernehmen, klicken Sie die Schaltfläche **[Submit]**.
Die Änderung der Authentifizierung wird nach dem nächsten Neustart wirksam.
Alle anderen Änderungen werden sofort wirksam.

15.1.1.2.19 Seite „SSH Server Settings“

Auf der Seite „SSH Server Settings“ finden Sie die Einstellungen zum SSH-Dienst.

Gruppe „SSH Server“

Tabelle 75: WBM-Seite „SSH Server Settings“ – Gruppe „SSH Server“

Parameter	Bedeutung
Service active	Hier schalten Sie den SSH-Server ein oder aus.
Port Number	Hier geben Sie die Port-Nummer ein.
Allow root login	Hier sperren oder erlauben Sie den Root-Zugriff.
Allow password login	Hier aktivieren oder deaktivieren Sie die Passwortabfrage.

Um die Änderungen zu übernehmen, klicken Sie die Schaltfläche **[Submit]**. Die Änderungen werden sofort wirksam.

15.1.1.2.20 Seite „DHCP Server Configuration“

Auf der Seite „DHCP Server Configuration“ finden Sie die Einstellungen zum DHCP-Dienst.

Gruppe „DHCP Server Configuration Bridge <n>“

Tabelle 76: WBM-Seite „DHCP Server Configuration“ – Gruppe „DHCP Configuration Bridge <n>“

Parameter	Bedeutung
Service active	Hier schalten Sie den DHCP-Dienst für das Interface X<n> ein oder aus.
Start IP for Range	Geben Sie hier den Anfangswert des verfügbaren IP-Adressbereichs ein.
End IP for Range	Geben Sie hier den Endwert des verfügbaren IP-Adressbereichs ein.
Lease time (min)	Hier geben Sie die Ausleihzeit in Minuten ein. Als Standardwert sind 120 Minuten eingetragen.
Static Hosts	Hier werden die statischen Zuordnungen von MAC-IDs zu IP-Adressen angezeigt. Wenn keine Zuordnung festgelegt wurde, wird „No static hosts configured“ angezeigt.
Add Static Host	Nachfolgend können Sie statische MAC-Adressen oder Hostnamen und IP-Adressen hinzufügen.
MAC Address or Hostname	Hier geben Sie eine neue statische Zuordnung ein, z. B. „01:02:03:04:05:06=192.168.1.20“ oder „hostname=192.168.1.20“. Sie können 15 Zuordnungen oder Hostnamen eintragen.
Ip Address	Hier geben Sie die IP-Adresse ein, Sie können 15 IP-Adressen eintragen.

Um die Änderungen zu übernehmen, klicken Sie die Schaltfläche **[Submit]**. Die Änderungen werden sofort wirksam.

Um eine neue Zuordnung zu übernehmen, klicken Sie die Schaltfläche **[Add]**. Die Änderung wird sofort wirksam.

Um eine bestehende Zuordnung zu löschen, klicken Sie die Schaltfläche **[Delete]**. Die Änderung wird sofort wirksam.

15.1.1.2.21 Seite „Configuration of DNS Server“

Auf der Seite „Configuration of DNS Server“ finden Sie die Einstellungen zum DNS-Dienst.

Gruppe „DNS Server“

Tabelle 77: WBM-Seite „Configuration of DNS Server“ – Gruppe „DNS Server“

Parameter	Bedeutung	
Service active	Hier schalten Sie den DNS-Server-Dienst ein oder aus.	
Mode	Hier wählen Sie die Betriebsart des DNS-Servers aus:	
	Proxy	Anfragen werden zur Durchsatzoptimierung zwischengespeichert.
	Relay	Alle Anfragen werden direkt weitergeleitet.
Static Hosts	Hier werden die statischen Zuordnungen von Namen zu IP-Adressen angezeigt. Wenn keine Zuordnung festgelegt wurde, wird „No static hosts configured“ angezeigt.	
Add Static Host	Nachfolgend können Sie statische IP-Adressen und Hostnamen hinzufügen.	
IP Address	Hier geben Sie eine neue feste Zuordnung ein, z. B. „192.168.1.20:hostname“. Sie können 10 Zuordnungen eintragen.	
Hostname	Hier geben Sie einen Hostnamen ein.	

Um die Änderungen zu übernehmen, klicken Sie die Schaltfläche **[Submit]**. Die Änderungen werden sofort wirksam.

Um eine neue Zuordnung zu übernehmen, klicken Sie die Schaltfläche **[Add]**. Die Änderung wird sofort wirksam.

Um eine bestehende Zuordnung zu löschen, klicken Sie die Schaltfläche **[Delete]**. Die Änderung wird sofort wirksam.

15.1.1.2.22 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 78: WBM-Seite „Overview“ – Gruppe „Connection <n>“

Parameter	Bedeutung
Is Active	Hier wird der Status der der Kommunikation mit der Cloud angezeigt.
Data from PLC Runtime	Hier wird angezeigt, wie viele Data-Collections seitens der IEC-Applikation für die Übertragung zur Cloud registriert wurden.
Cloud Connection	Hier wird der Status der Verbindung zum Cloud-Dienst angezeigt.
Heartbeat	Hier wird das aktuell konfigurierte Heartbeat-Intervall in Sekunden angezeigt.
Telemetry data transmission	Hier wird angezeigt, ob die Übertragung von Daten aktiviert oder deaktiviert ist.
Cache fill level (QoS 1 and 2)	Hier wird der Füllstand des Speichers für ausgehende Nachrichten in Prozent angezeigt.

Gruppe „Diagnosis“

Diese Gruppe ist nur sichtbar, wenn Diagnoseinformationen vorliegen.

Hier werden Warnungen und Fehler angezeigt sowie Informationen (sofern verfügbar) zur möglichen Fehlerbehebung.

15.1.1.2.23 Seite „Configuration of Connection <n>“

Auf der Seite „Configuration of Connection <n>” finden Sie Einstellungen und Informationen zum Cloud-Zugang.

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 separaten Tabellen dargestellt.

Tabelle 79: WBM-Seite „Configuration of Connection <n>“ – Gruppe „Configuration“

Parameter	Bedeutung
Enabled	Hier aktivieren/deaktivieren Sie die Cloud-Connectivity-Funktionalität.
Cloud platform	Hier wählen Sie die Cloud-Plattform aus.
Hostname	Hier geben Sie den Hostnamen oder die IP-Adresse für die ausgewählte Cloud-Plattform ein.
ID Scope	Hier geben Sie den Endpunkt für den Azure Gerätebereitstellungsdienst (DPS) ein
Registration ID	Hier geben Sie die Registrierungs-ID für den Azure Gerätebereitstellungsdienst (DPS) ein.
Port number	Hier geben Sie den Port ein, zu dem eine Verbindung aufgebaut werden soll. Typische Werte sind 8883 für verschlüsselte Verbindungen und 1883 für unverschlüsselte Verbindungen.
Device ID	Hier geben Sie die Device-ID für die ausgewählte Cloud-Plattform ein.
Client ID	Hier geben Sie die Client-ID für die ausgewählte Cloud-Plattform ein.
Authentication	Hier wählen Sie die Authentifizierungsmethode aus. Mögliche Einstellungen sind „Shared Key Acces“ oder „X.509 Certificate“.
Activation Key	Hier geben Sie den Aktivierungsschlüssel für die ausgewählte Cloud-Plattform ein.
Clean Session	Hier geben Sie an, ob Clean-Session bei der Verbindung zum Cloud-Dienst aktiv sein soll. Wenn Clean-Session aktiv ist, werden die Informationen und Nachrichten zu dieser Verbindung beim Cloud-Dienst nicht persistent gespeichert.
TLS	Hier stellen Sie ein, ob die TLS-Verschlüsselung für die Verbindung zur Cloud-Plattform verwendet werden soll. Amazon Web Services (AWS) verwendet immer TLS.

Tabelle 79: WBM-Seite „Configuration of Connection <n>“ – Gruppe „Configuration“

Parameter	Bedeutung
CA file	Hier geben Sie den Pfad zu der im PEM-Format enkodierten Datei ein, die das für den Aufbau einer verschlüsselten Verbindung zu verwendende und vertrauenswürdige CA-Zertifikat enthält. Standardwert ist das bereits auf dem Controller installierte CA-Zertifikat /etc/ssl/certs/ca-certificates.crt.
User	Hier geben Sie den Benutzernamen für die Authentisierung gegenüber dem Cloud-Dienst ein.
Password	Hier geben Sie das Passwort für die Authentisierung gegenüber dem Cloud-Dienst ein.
Certification file	Hier geben Sie den Pfad zu der im PEM-Format enkodierten Datei ein, die zur Authentisierung gegenüber dem Cloud-Dienst genutzt wird.
Key file	Hier geben Sie den Pfad zu der im PEM-Format enkodierten Datei ein, welche den privaten Schlüssel für die Authentisierung gegenüber dem Cloud-Dienst enthält.
Use websockets	Hier stellen Sie ein, ob die Verbindung zur Cloud-Plattform mittels Websocket-Protokoll über den Port 443 aufgebaut werden soll. Wenn das Kontrollfeld deaktiviert ist, wird die Verbindung zur Cloud-Plattform mittels MQTT-Protokoll über den Port 8883 aufgebaut.
Proxy Type	Hier wählen Sie aus, welche Art von Proxy genutzt werden soll.
HTTP Proxy Host	Hier geben Sie den Hostnamen oder die IP-Adresse des Proxys ein.
HTTP Proxy Port	Hier geben Sie die Portnummer des Proxys ein.
HTTP Proxy User	Hier geben Sie den Namen des Proxy-Benutzers ein.
HTTP Proxy Password	Hier geben Sie das Passwort des Proxy-Benutzers ein.
Use compression	Hier stellen Sie ein, ob die Daten mittels GZIP-Komprimierung komprimiert werden.
Data Protocol	Hier wählen Sie das Daten-Protokoll aus.
Cache mode	Hier stellen Sie ein, in welchem Speicher der Cache für die Datentelegramme angelegt werden soll. Dieses Auswahlfeld ist nur aktiv, wenn eine korrekt formatierte SD-Karte gesteckt ist. (Weitere Informationen finden Sie im Anwendungshinweis A500920.)
Last Will	Hier stellen Sie ein, ob eine Last-Will-Nachricht aktiviert/deaktiviert sein soll.
(Last Will) Topic	Hier geben Sie das Topic ein, unter welchem die Last-Will-Nachricht versendet werden soll.

Tabelle 79: WBM-Seite „Configuration of Connection <n>“ – Gruppe „Configuration“

Parameter	Bedeutung
(Last Will) Message	Hier geben Sie die Nachricht ein, welche Sie als Last-Will-Nachricht versenden wollen.
(Last Will) QoS	Hier geben Sie den „Quality of Service“ (QoS) der Last-Will-Nachricht an.
(Last Will) Retain	Hier stellen Sie ein, ob die letzte unter einem Topic gesendete Last-Will-Nachricht vom Broker als gespeicherte Nachricht (Retained Message) behandelt werden soll.
Device info	Hier stellen Sie ein, ob eine Device-Info-Nachricht erzeugt wird, welche den Cloud-Dienst über die grundlegende Konfiguration des Controllers informiert. (Weitere Informationen finden Sie im Anwendungshinweis A500920.)
Device status	Hier stellen Sie ein, ob Device-State-Nachrichten erzeugt werden sollen, welche den Cloud-Dienst über Änderungen des Betriebsartenschalters sowie der LEDs informiert. (Weitere Informationen finden Sie im Anwendungshinweis A500920.)
Standard commands	Hier stellen Sie ein, ob die integrierten Standardkommandos unterstützt werden sollen. (Die Liste der Standardkommandos finden Sie im Anwendungshinweis A500920.) Wenn das Kontrollfeld deaktiviert ist, werden nur die im IEC-Programm definierten Kommandos unterstützt.
Application property template	Hier haben Sie die Möglichkeit ein eigenes Property für die einzelnen MQTT Nachrichten zur Azure-Cloud erstellen. Dieser Parameter ist optional, d. h., wenn das Feld leer gelassen wird, wird dieses Property nicht mitgesendet. Zur Erstellung dieses Properties stehen die folgenden Platzhalter zur Verfügung: • <m>: Nachrichtentype • <p>: Protokoll-Version • <d>: DeviceId Beispiele: • MyKey=HelloWorld_<m> • TestKey=<m>/<p>/<d> • DeviceId=<d>

Um eine Änderung zu übernehmen, klicken Sie die Schaltfläche **[Submit]**.

Die Änderungen werden erst nach dem nächsten Neustart des Controllers wirksam. Nutzen Sie hierzu die Reboot-Funktion des WBM. Schalten Sie den Controller nicht zu früh aus!

Die nachfolgenden Tabellen zeigen die Abhängigkeiten der Auswahl- und Eingabefelder sowie der möglichen Einstellungen.

Tabelle 80: Anzeige der Auswahl- und Eingabefelder abhängig von der ausgewählten Cloud-Plattform

Auswahl- oder Eingabefeld	Cloud-Plattform					
	WAGO Cloud	Azure	MQTT AnyCloud	Amazon Web Services	SAP IoT Services	Azure Device Provisioning Service (DPS)
Enabled	X	X	X	X	X	X
Cloud platform	X	X	X	X	X	X
Hostname	X	X	X	X	X	
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	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

Tabelle 80: Anzeige der Auswahl- und Eingabefelder abhängig von der ausgewählten Cloud-Plattform

Auswahl- oder Eingabefeld	Cloud-Plattform					
	WAGO Cloud	Azure	MQTT AnyCloud	Amazon Web Services	SAP IoT Services	Azure Device Provisioning Service (DPS)
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 81: Auswahlmöglichkeit des Datenprotokolls abhängig von der ausgewählten Cloud-Plattform

Datenprotokoll	**Cloud-Plattform**					
	WAGO Cloud	**Azure**	**MQTT AnyCloud**	**Amazon Web Services**	**SAP IoT Services**	**Azure Device Provisioning Service (DPS)**
WAGO Protocol		X	X	X		X
WAGO Protocol 1.5		X	X	X		X
Native MQTT			X	X	(X)	
Sparkplug payload B		X	X	X		

X: Auswahl möglich
(X): Fest eingestellt

Tabelle 82: 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 83: 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 84: 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

15.1.1.2.24 Seite „Configuration of General SNMP Parameters“

Auf der Seite „Configuration of General SNMP Parameters“ finden Sie allgemeine Einstellungen zu SNMP.

Gruppe „General SNMP Configuration“

Tabelle 85: WBM-Seite „Configuration of General SNMP Parameters“ – Gruppe „General SNMP Configuration“

Parameter	Bedeutung
Service active	Hier aktivieren/deaktivieren Sie den SNMP-Service.
Name of Device	Hier geben Sie den Gerätenamen (sysName) ein.
Description	Hier geben Sie die Gerätebeschreibung (sysDescription) ein.
Physical Location	Hier geben Sie den Standort des Gerätes (sysLocation) ein.
Contact	Hier geben Sie die E-Mail-Kontaktadresse (sysContact) ein.
ObjectID	Hier geben Sie die Object-ID ein.

Um die Änderungen zu übernehmen, klicken Sie die Schaltfläche **[Submit]**.

15.1.1.2.25 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 86: WBM-Seite „Configuration of SNMP v1/v2c Parameters“ – Gruppe „Communities“

Parameter	Bedeutung
Community <n>	Für jede konfigurierte Community wird ein eigener Bereich angezeigt. Wenn keine Community konfiguriert wurde, wird „(no Communities configured)“ angezeigt.
Name	Anzeige des Community-Namens für die SNMP-Manager-Konfiguration. Über den Community-Namen können Beziehungen zwischen SNMP-Managern und -Agenten eingerichtet werden, die jeweils als Community bezeichnet werden und die Identifizierung sowie den Zugriff zwischen den SNMP-Teilnehmern steuern.
Access	Hier werden die Zugriffsrechte für die Community angezeigt. Mögliche Werte sind: „ReadOnly“ oder „ReadWrite“.
Add new Community	In diesem Bereich können Sie eine neue Community hinzufügen.
Name	Hier geben Sie den Community-Namen für die neue SNMP-Manager-Konfiguration ein (s. o.). Der Community-Name darf maximal 32 Zeichen lang sein und keine Leerzeichen enthalten. Um das SNMP-Protokoll verwenden zu können, muss immer ein gültiger Community-Name angegeben sein. Standard ist „public“.
Access	Hier wählen Sie die Zugriffsrechte für die neue Community aus. Mögliche Werte sind: „ReadOnly“ oder „ReadWrite“.

Um eine bestehende Community zu löschen, klicken Sie die entsprechende Schaltfläche **[Delete]**.

Um eine neue Community hinzuzufügen, klicken Sie die Schaltfläche **[Add]**.

Gruppe „Trap Receivers“

Tabelle 87: WBM-Seite „Configuration of SNMP v1/v2c Parameters“ – Gruppe „Trap Receivers“

Parameter	Bedeutung
Trap Receiver <n>	Für jeden konfigurierten Trap-Empfänger wird ein eigener Bereich angezeigt. Wenn kein Trap-Empfänger konfiguriert wurde, wird „(no Trap Receivers configured)“ angezeigt.
Host	Hier wird der Host-Name oder die IP-Adresse des Trap-Empfängers (Managementstation) angezeigt.
Community Name	Hier wird der Community-Name für die Trap-Empfänger-Konfiguration angezeigt. Der Community-Name kann durch den Trap-Empfänger ausgewertet werden.
Version	Hier wird die SNMP-Version angezeigt, über welche die Traps gesendet werden sollen.
Add new Trap Receiver	In diesem Bereich können Sie einen neuen Trap-Empfänger hinzufügen.
Host	Hier geben Sie den Host-Namen oder die IP-Adresse des neuen Trap-Empfängers (Managementstation) ein.
Community Name	Hier geben Sie den Community-Namen für die neue Trap-Empfänger-Konfiguration an (s.o.). Der Community-Name darf maximal 32 Zeichen lang sein und keine Leerzeichen enthalten.
Version	Hier wählen Sie die SNMP-Version aus, über welche die Traps gesendet werden sollen. Mögliche Werte: „v1“ oder „v2c“.

Um einen bestehenden Trap-Empfänger zu löschen, klicken Sie die entsprechende Schaltfläche **[Delete]**.

Um einen neuen Trap-Empfänger hinzuzufügen, klicken Sie die Schaltfläche **[Add]**.

15.1.1.2.26 Seite „Configuration of SNMP v3 Parameters“

Auf der Seite „Configuration of SNMP v3 Parameters“ finden Sie die Einstellungen zu SNMP v3.

Gruppe „Users“

Tabelle 88: WBM-Seite „Configuration of SNMP v3 Parameters“ – Gruppe „Users“

Parameter	Bedeutung
User <n>	Für jeden konfigurierten v3-User wird ein eigener Bereich angezeigt. Wenn kein v3-User konfiguriert wurde, wird „(no Users configured)“ angezeigt.
Security Authentication Name	Hier wird der Benutzername angezeigt.
Authentication Type	Hier wird der Authentifizierungstyp für die SNMP-v3-Pakete angezeigt. Mögliche Werte sind: - Keine Authentifizierung benutzen („None“) - Message Digest 5 („MD5“) - Secure Hash Algorithm („SHA“, “SHA224”, “SHA256”, “SHA384”, “SHA512”)
Authentication Key	Hier wird der Schlüssel für die Authentifizierung angezeigt.
Privacy	Hier wird der Verschlüsselungsalgorithmus für die SNMP-Nachricht angezeigt. Mögliche Werte sind: - Keine Verschlüsselung („None“) - Data Encryption Standard („DES“) - Advanced Encryption Standard („AES“, “AES128”, “AES192”, “AES192C”, “AES256”, “AES256C”)
Privacy Key	Hier wird der Schlüssel für die Verschlüsselung der SNMP-Nachricht angezeigt. Wird hier nichts angezeigt, dann wird automatisch der „Authentication Key“ verwendet.
Access	Hier werden die Zugriffsrechte für den User angezeigt. Mögliche Werte sind: „ReadOnly“ oder „ReadWrite“.
Add new v3 User	In diesem Bereich können Sie einen neuen v3-User anlegen. Sie können maximal 10 User anlegen.
Security Authentication Name	Hier geben Sie den Benutzernamen ein. Dieser muss eindeutig sein; ein bereits vorhandener Benutzername wird bei der Neueingabe nicht akzeptiert. Der Name darf min. 8 und max. 32 Zeichen lang sein und Kleinbuchstaben (a … z), Großbuchstaben (A … Z), Ziffern (0 … 9), die Sonderzeichen !()*~'.-_ aber keine Leerzeichen enthalten.

Tabelle 88: WBM-Seite „Configuration of SNMP v3 Parameters“ – Gruppe „Users“

Parameter	Bedeutung
Authentication Type	Hier geben Sie den Authentifizierungstyp für die SNMP-v3-Pakete ein. Mögliche Werte sind: - Keine Authentifizierung benutzen („None“) - Message Digest 5 („MD5“) - Secure Hash Algorithm („SHA“, “SHA224”, “SHA256”, “SHA384”, “SHA512”)
Authentication Key	Hier geben Sie den Schlüssel für die Authentifizierung ein. Der Schlüssel darf min. 8 und max. 32 Zeichen lang sein und Kleinbuchstaben (a … z), Großbuchstaben (A … Z), Ziffern (0 … 9), die Sonderzeichen !()*~'.-_ aber keine Leerzeichen enthalten.
Privacy	Hier geben Sie einen Verschlüsselungsalgorithmus für die SNMP-Nachricht ein. Mögliche Werte sind: - Keine Verschlüsselung („None“) - Data Encryption Standard („DES“) - Advanced Encryption Standard („AES“, “AES128”, “AES192”, “AES192C”, “AES256”, “AES256C”)
Privacy Key	Hier geben Sie den Schlüssel für die Verschlüsselung der SNMP-Nachricht ein. Wenn Sie hier nichts eingeben, dann wird automatisch der „Authentication Key“ verwendet. Der Schlüssel darf min. 8 und max. 32 Zeichen lang sein und Kleinbuchstaben (a … z), Großbuchstaben (A … Z), Ziffern (0 … 9), die Sonderzeichen !()*~'.-_ aber keine Leerzeichen enthalten.
Access	Hier wählen Sie die Zugriffsrechte für den neuen User aus. Mögliche Werte sind: „ReadOnly“ oder „ReadWrite“.

Um einen bestehenden User zu löschen, klicken Sie die entsprechende Schaltfläche **[Delete]**.

Um einen neuen User hinzuzufügen, klicken Sie die Schaltfläche **[Add]**.

Gruppe „Trap Receivers“

Tabelle 89: WBM-Seite „Configuration of SNMP v3 Parameters“ – Gruppe „Trap Receivers“

Parameter	Bedeutung
Trap Receiver <n>	Für jeden konfigurierten v3-Trap-Empfänger wird ein eigener Bereich angezeigt. Wenn kein v3-Trap-Empfänger konfiguriert wurde, wird „(no Trap Receivers configured)“ angezeigt.
Security Authentication Name	Hier wird der Benutzername angezeigt.
Authentication Type	Hier wird der Authentifizierungstyp für die SNMP-v3-Pakete angezeigt. Mögliche Werte sind: - Keine Authentifizierung benutzen („None“) - Message Digest 5 („MD5“) - Secure Hash Algorithm („SHA“, “SHA224”, “SHA256”, “SHA384”, “SHA512”)
Authentication Key	Hier wird der Schlüssel für die Authentifizierung angezeigt.
Privacy	Hier wird der Verschlüsselungsalgorithmus für die SNMP-Nachricht angezeigt. Mögliche Werte sind: - Keine Verschlüsselung („None“) - Data Encryption Standard („DES“) - Advanced Encryption Standard („AES“, “AES128”, “AES192”, “AES192C”, “AES256”, “AES256C”)
Privacy Key	Hier wird der Schlüssel für die Verschlüsselung der SNMP-Nachricht angezeigt. Wird hier nichts angezeigt, dann wird automatisch der „Authentication Key“ verwendet.
Host	Hier wird der Hostname oder die IP-Adresse eines Trap-Empfängers für v3-Traps angezeigt.
Add new Trap Receiver	In diesem Bereich können Sie einen neuen v3-Trap-Empfänger anlegen. Sie können maximal 10 Trap-Empfänger anlegen.
Security Authentication Name	Hier geben Sie den Benutzernamen ein. Dieser muss eindeutig sein; ein bereits vorhandener Benutzername wird bei der Neueingabe nicht akzeptiert. Der Name darf min. 8 und max. 32 Zeichen lang sein und Kleinbuchstaben (a … z), Großbuchstaben (A … Z), Ziffern (0 … 9), die Sonderzeichen !()*~'.-_ aber keine Leerzeichen enthalten.

Tabelle 89: WBM-Seite „Configuration of SNMP v3 Parameters“ – Gruppe „Trap Receivers“

Parameter	Bedeutung
Authentication Type	Hier geben Sie den Authentifizierungstyp für die SNMP-v3-Pakete ein. Mögliche Werte sind: - Keine Authentifizierung benutzen („None“) - Message Digest 5 („MD5“) - Secure Hash Algorithm („SHA“, “SHA224”, “SHA256”, “SHA384”, “SHA512”)
Authentication Key	Hier geben Sie den Schlüssel für die Authentifizierung ein. Der Schlüssel darf min. 8 und max. 32 Zeichen lang sein und Kleinbuchstaben (a … z), Großbuchstaben (A … Z), Ziffern (0 … 9), die Sonderzeichen !()*~'.-_ aber keine Leerzeichen enthalten.
Privacy	Hier geben Sie einen Verschlüsselungsalgorithmus für die SNMP-Nachricht ein. Mögliche Werte sind: - Keine Verschlüsselung („None“) - Data Encryption Standard („DES“) - Advanced Encryption Standard („AES“, “AES128”, “AES192”, “AES192C”, “AES256”, “AES256C”)
Privacy Key	Hier geben Sie den Schlüssel für die Verschlüsselung der SNMP-Nachricht ein. Wenn Sie hier nichts eingeben, dann wird automatisch der „Authentication Key“ verwendet. Der Schlüssel darf min. 8 und max. 32 Zeichen lang sein und Kleinbuchstaben (a … z), Großbuchstaben (A … Z), Ziffern (0 … 9), die Sonderzeichen !()*~'.-_ aber keine Leerzeichen enthalten.
Host	Hier geben Sie den Hostnamen oder die IP-Adresse eines Trap-Empfängers für v3-Traps ein.

Um einen bestehenden User zu löschen, klicken Sie die entsprechende Schaltfläche **[Delete]**.

Um einen neuen User hinzuzufügen, klicken Sie die Schaltfläche **[Add]**.

15.1.1.2.27 Seite „Favorites“

Auf der Seite „Favorites“ können Sie die Startseite des Produktes einstellen. Außerdem hält diese Seite eine Liste einstellbarer Controller für Sie bereit.

Für die Startseite können Sie aus der verfügbaren Liste einen bestimmten Controller auswählen, der beim Einschalten des Produktes angezeigt wird.

Wenn eine Webseite oder ein Controller als Startseite ausgewählt wurde, wird, unabhängig davon, ob ein Boot-Projekt vorhanden ist oder nicht, die Webseite bzw. der Controller als Startseite angezeigt.

Wenn das WBM oder „Browser Favorites“ als Startseite aktiviert wurde und ein Boot-Projekt vorhanden ist, wird die Target-Visualisierung als Startseite angezeigt.

Wenn das WBM oder „Browser Favorites“ als Startseite aktiviert wurde und kein Boot-Projekt vorhanden ist, wird das WBM bzw. werden die „Browser Favorites“ als Startseite angezeigt.

Hinweis

Bei vorhandener Target-Visualisierung ist kein Einstellen einer Startseite möglich!
Wenn auf dem Produkt eine Target-Visualisierung projektiert und gestartet wurde, hat die Auswahl einer Startseite keine Auswirkungen, weil direkt die Target-Visualisierung gestartet wird.

Gruppe „WBM“

Hier aktivieren/deaktivieren Sie das WBM als Startseite, die beim Einschalten des Produktes angezeigt wird.

Um eine Änderung zu übernehmen, klicken Sie die Schaltfläche **[Submit]**.

Gruppe „Browser Favorites“

Hier aktivieren/deaktivieren Sie die „Browser Favorites“-Auswahlliste als Startseite, die beim Einschalten des Produktes angezeigt wird.

Um eine Änderung zu übernehmen, klicken Sie die Schaltfläche **[Submit]**.

Gruppen „Favorite n“

Jede Gruppe beschreibt die Verbindung zu einem bestimmten Controller. Wird der Name eines Controllers geändert, so wird dieser Name auch zur neuen Gruppenbezeichnung.

Hier aktivieren/deaktivieren einen Favoriten als Startseite, die beim Einschalten des Produktes angezeigt wird.

Hier aktivieren/deaktivieren Sie den MicroBrowser für den bestimmten Controller.

Tabelle 90: WBM-Seite „Favorites ” – Gruppen „Favorite n“

Parameter	Bedeutung
Startpage	Aktivieren/deaktivieren Sie diesen Favoriten als Startseite, die beim Einschalten des Produktes angezeigt wird.
Name	Vergeben Sie einen beliebigen Namen für den Controller.
URL	Geben Sie die URL an, unter der die Webvisualisierung des Controllers erreichbar ist.
Virtual Keyboard	Legen Sie fest, ob bei Anzeige der URL dieses Controllers die virtuelle Paneltastatur verwendet werden soll. Dies ist sinnvoll, wenn Sie z. B. eine WebVisu anzeigen möchten, für welche eine eigene virtuelle Tastatur erforderlich ist.
WebVisu	Legen Sie fest, ob es sich bei der angegebenen URL um eine WebVisu handelt oder nicht.
MicroBrowser	Aktivieren/deaktivieren Sie den MicroBrowser für den Controller.

Um eine Änderung zu übernehmen, klicken Sie die Schaltfläche **[Submit]**. Um alle Eingabefelder des Eintrags zurückzusetzen, klicken Sie die Schaltfläche **[Clear]**. Bestätigen Sie das Zurücksetzen mit **[Submit]**.

Die Aktivierung/Deaktivierung des MicroBrowsers 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!

Hinweis

CODESYS V3-Applikation verhindert Webvisualisierung durch den MicroBrowser!
Für die Aktivierung des MicroBrowsers darf keine CODESYS V3-Applikation auf dem Produkt aufgespielt sein.

Bei einer gestörten oder unterbrochenen Verbindung von Browser zur Steuerung wird im MicroBrowser ein orangefarbenes Rechteck mit einem Ausrufezeichen angezeigt.

Wenn beim Starten des Produktes die Gegenstelle (PLC) noch nicht verfügbar ist, wird ein Startbild angezeigt.

Für den MicroBrowser gelten die Standard-Anmeldedaten:

Tabelle 91: MicroBrowser – Anmeldedaten

Benutzer	Standardpasswort
admin	wago

15.1.1.2.28 Seite „Autostart“

Auf dieser Seite können Sie die Autostart-Optionen für die Runtime einstellen.

Gruppe „Autostart“

Stellen Sie hier den Countdown ein, der beim Hochfahren vor dem Anzeigen der Startseite angezeigt wird. Innerhalb des eingestellten Zeitraums haben Sie dann die Möglichkeit, den automatischen Wechsel zur Startseite zu verhindern und an dieser Stelle direkt zum WBM zu wechseln. Ein Delay „0“ zeigt direkt die Startseite an.

15.1.1.2.29 Seite „Monitoring“

Auf der Seite „Monitoring“ finden Sie die Einstellungen zur Überwachung des Produktes.

Gruppe „Monitoring“

Tabelle 92: WBM-Seite „Monitoring” – Gruppe „Monitoring“

Parameter	Bedeutung
Reconnect	Legen Sie fest, ob nach einer Verbindungsunterbrechung zum Produkt automatisch versucht werden soll, die Verbindung wiederherzustellen.
Interval (s)	Geben Sie ein Intervall für die Versuche an.

15.1.1.2.30 Seite „Browser Security“

Auf der Seite „Browser Security“ legen Sie die Sicherheitsstufe des Browsers fest.

Gruppe „Browser Security“

Wählen Sie die gewünschte Sicherheitsstufe aus (Low oder High).

Tabelle 93: WBM-Seite „Browser Security” – Gruppe „ Browser Security “

Parameter	Bedeutung
Browser Security	• Low: In dieser Sicherheitsstufe werden HTTPS-Verbindungen mit: •• Zertifikaten, die noch nicht gültig sind, •• Zertifikaten, die abgelaufen sind, •• Zertifikaten, die selbst signiert sind und •• Zertifikaten mit nicht übereinstimmenden Hostnamen zugelassen. • High: In dieser Sicherheitsstufe werden die oben aufgelisteten, in „Low“ zugelassenen Verbindungen abgelehnt.

15.1.1.2.31 Seite „Commissioning Settings“

Auf der Seite „Commissioning Settings“ kann der Commissioning-Agent aktiviert bzw. deaktiviert werden. Außerdem können Statusinformation ausgelesen werden. Im aktiven Zustand sucht der Commissioning-Agent nach jedem Neustart des Controllers fünf Minuten lang nach einem Server.

Gruppe „Commissioning“

Tabelle 94: WBM-Seite „Commisioning Settings“ – Gruppe „Commissioning“

Parameter	Bedeutung	
Service Enabled	Hier aktivieren/deaktivieren Sie den „Commissioning Agent“-Dienst:	
	Deaktiviert	Der „Commissioning Agent“-Dienst ist deaktiviert.
	Aktiviert	Der „Commissioning Agent“-Dienst ist aktiviert.
Commissioning State	Hier wird der aktuelle Status des „Commissioning Agent“-Dienstes angezeigt.	
	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.
	success	Der Dienst hat die Installation erfolgreich abgeschlossen.
Connected Server	Hier wird die Domain des Servers, mit dem das Produkt verbunden ist, angezeigt; Ist das Produkt nicht verbunden, wird „-“ angezeigt.	

Um die Änderungen zu übernehmen, klicken Sie die Schaltfläche **[Submit]**. Die Änderungen werden sofort wirksam.

15.1.1.2.32 Seite „Docker Settings“

Auf der Seite „Docker Settings“ finden Sie die Einstellungen zum Dienst „Docker®“.

Gruppe „Docker Status“

Tabelle 95: WBM-Seite „Docker Settings“ – Gruppe „Docker Status“

Parameter	Bedeutung	
Current State	Hier wird der aktuelle Status des Dienstes „Docker®“ angezeigt.	
	stopped	Der Dienst „Docker®“ ist nicht aktiv.
	running	Der Dienst „Docker®“ ist aktiv.
Service Enabled	Wenn Sie den Dienst „Docker®“ aktivieren wollen, markieren Sie dieses Kontrollfeld.	

Um die Änderungen zu übernehmen, klicken Sie die Schaltfläche **[Submit]**. Die Änderungen werden sofort wirksam.

15.1.1.2.33 Seite „Fonts“

Auf dieser Seite können Sie Schriftarten von einem PC aus hochladen oder löschen.

Klicken Sie in das Feld „Choose file…“. Wählen Sie die gewünschte True Type Font-Datei (*.ttf) aus.

Klicken Sie die Schaltfläche **[Upload]**, um die Schrift hochzuladen. In der Liste oberhalb des Feldes „Choose file…“ erscheint die hochgeladene Schriftart. Die Schriftart steht erst nach dem nächsten Neustart zur Verfügung.

Klicken Sie die Schaltfläche **[Delete]**, um eine Schriftart zu löschen.

15.1.1.2.34 Seite „Display Orientation“

Auf der Seite „Display Orientation“ können Sie Einstellungen zur Displayausrichtung treffen.

Gruppe „Display Orientation“

Stellen Sie ein, ob das Display im Hoch- oder Querformat angezeigt werden soll. Die Optionen sind landscape, portrait, landscape rotated und portrait rotated.

15.1.1.2.35 Seite „Screensaver“

Auf der Seite „Screensaver“ können Sie den Bildschirmschoner (Screensaver) anpassen.

Gruppe „Screensaver Settings“

Stellen Sie ein, ob und wie ein Bildschirmschoner verwendet werden soll.

Tabelle 96: WBM-Seite „Screensaver ” – Gruppe „Screensaver Settings“

Parameter	Bedeutung
Enabled	Hier können Sie den Bildschirmschoner aktivieren bzw. deaktivieren.
Setting	Geben Sie an, ob ein Bild, die Uhrzeit, ein Text oder ein „Backlight” angezeigt werden soll oder ob „Screen care“ (Bildschirmpflege) durchgeführt werden soll. • Image: Der Bildschirmschoner wird mit dem WAGO Logo nach der unter „Duration“ eingestellten Zeit aktiviert. • Text: Geben Sie hier einen Text ein, der nach Ablauf der unter „Duration“ eingestellten Zeit als Bildschirmschoner aktiviert wird. • Time: Als Bildschirmschoner wird die aktuelle Uhrzeit zur Anzeige gebracht. • Backlight: Die Helligkeit wird auf die Bildschirmschoner-Helligkeit reduziert und das WAGO Logo angezeigt. • Screen care: Zur Bildschirmpflege werden alle Pixel für einige Millisekunden invertiert (nicht sichtbar). • Off: Es soll kein Bildschirmschoner angezeigt werden.
Text	Geben Sie hier einen beliebigen Text zur Anzeige für den Text-Bildschirmschoner ein. (einstellbar bei Option „Text“.)
Duration (s)	Wenn das Display nicht bedient wird, wird nach Ablauf der hier eingestellten Zeit der Bildschirmschoner aktiviert.

Gruppe „Screen Care“

Stellen Sie ein, wie lange das Display bei Ausführung einer Reinigung inaktiv geschaltet werden soll.

Tabelle 97: WBM-Seite „Screensaver ” – Gruppe „Screen Care“

Parameter	Bedeutung
Enabled	Hier können Sie die Bildschirmpflege aktivieren bzw. deaktivieren.
Time (hh:mm:ss)	Geben Sie hier die Uhrzeit ein, zu der eine Bildschirmpflege durchgeführt werden soll. (Einstellbar bei Option „Screen care“.)

15.1.1.2.36 Seite „WBM User Configuration“

Auf der Seite „WBM User Configuration“ finden Sie die Einstellungen zur User-Aministration.

Gruppe „Change Password“

Hinweis

Passwörter ändern
Die im Auslieferungszustand eingestellten Initialpasswörter sind in diesem Handbuch dokumentiert und bieten daher keinen hinreichenden Schutz! Ändern Sie die Passwörter entsprechend Ihren Erfordernissen!

Tabelle 98: WBM-Seite „WBM User Configuration” – Gruppe „Change Password“

Parameter	Bedeutung
Old Password	Hier geben Sie zur Authentifizierung das aktuell verwendete Passwort ein.
New Password	Hier geben Sie das neue Passwort ein. Zulässige Zeichen für das Passwort sind folgende ASCII-Zeichen: a … z, A … Z, 0 … 9, und die Sonderzeichen: !"#$%&'()*+,./:;<=>?@[]^_`{}|~-.
Confirm Password	Hier geben Sie zur Kontrolle das neue Passwort erneut ein.

Um eine Änderung zu übernehmen, klicken Sie die Schaltfläche **[Submit]**. Die Änderung wird sofort wirksam.

Hinweis

Zulässige Zeichen für WBM-Passwörter beachten!
Werden außerhalb des WBM (z. B. über eine USB-Tastatur) Passwörter mit unzulässigen Zeichen für das WBM eingestellt, ist ein Zugriff auf die Seiten direkt am Display nicht mehr möglich, da nur die zulässigen Zeichen über die virtuelle Tastatur zur Verfügung stehen!

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.

Die Benutzerverwaltung für die Steuerungsanwendungen wird separat angelegt und verwaltet.

15.1.1.3 Registerkarte „Fieldbus“

15.1.1.3.1 Seite „OPC UA Configuration“

Auf der Seite „OPC UA Configuration“ finden Sie die Einstellungen zum OPC-UA-Dienst.

Gruppe „OPC UA Server Configuration“

Tabelle 99: WBM-Seite „OPC UA Configuration“ – Gruppe „OPC UA Server Configuration“

Parameter	Bedeutung
Enabled	Hier aktivieren oder deaktivieren Sie den OPC-UA-Server.
Log Level	Hier wählen Sie den Log-Level aus. Folgende Werte sind einstellbar: Error / Warning / Info / Debug. Mit dem Log-Level „Error“ werden nur Fehlermeldungen ausgegeben, mit dem Log-Level „Info“ auch Statusmeldungen. 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.
Ctrl Configuration name	Hier geben Sie den Konfigurationsnamen an, den der Controller innerhalb des PLC Open Device Sets erhält.

Um die Änderungen zu übernehmen, klicken Sie die Schaltfläche **[Submit]**.

Gruppe „OPC UA Server Security Settings“

Tabelle 100: WBM-Seite „OPC UA Configuration“ – Gruppe „OPC UA Server Security Settings“

Parameter	Bedeutung
Anonymous Access	Anonymen Zugriff auf den Server zulassen Dies setzt voraus, dass die Portauthentifizierung der Runtime ebenfalls deaktiviert ist/wird.
Allow Password On Plaintext	Übertragung des Passworts im lesbaren Format
Security Modes	Security Mode des OPC UA Servers Je nach Auswahl der Betriebsart stehen Ihnen verschiedene OPC UA Endpoints zum Verbindungsaufbau zu Verfügung: None: Lediglich der OPC UA Endpoint **None** wird aktiviert. Dieser ermöglicht eine ungesicherte Verbindung zum OPC UA Server. None + Sign + SignAndEncrypt: Die Enpoints **None**, **Sign** und **SignAndEncrypt** stehen zur Verfügung. **Sign** stellt einen Endpoint zur Verfügung, welcher über ein Passwort geschützt ist. **SignAndEncrypt** stellt einen Endpoint zur Verfügung, welcher neben einem Passwort auch eine Verschlüsselung zur Verfügung stellt. Sign + SignAndEncrypt: Die Endpoints **Sign** sowie **SignAndEncrypt** stehen zur Verfügung. SignAndEncrypt: Lediglich der Endpoint **SignAndEncrypt** 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.

Um die Änderungen zu übernehmen, klicken Sie die Schaltfläche **[Submit]**.

15.1.1.3.1 Seite „BACnet Status“

Auf der Seite „BACnet Status” werden für den Feldbus BACnet und die BACnet-Lizenz spezifische Informationen über Ihren Controller angezeigt.

Gruppe „BACnet Information“

Tabelle 101: WBM-Seite „BACnet Status” – Gruppe „BACnet Information“

Parameter	Bedeutung
State	Hier wird angezeigt, ob der Feldbus BACnet aktiviert (enabled) oder deaktiviert (disabled) ist.
Mode	Hier wird der Betriebsmodus des Feldbusses angezeigt (ip / sc).
Version	Hier wird die installierte BACnet Version angezeigt.
Status Info	Hier wird der Status des Feldbusses BACnet angezeigt.
Device-ID	Hier wird die aktuelle Device-ID des Controllers angezeigt.

Gruppe „BACnet License“

Tabelle 102: WBM-Seite „BACnet Status” – Gruppe „BACnet License“

Parameter	Bedeutung
Type	Hier werden die BACnet Lizenzen angezeigt.
User Objects	Hier wird die Anzahl der vorhandenen sowie der mit der Lizenz möglichen BACnet-Objekte angezeigt.

Gruppe „BACnet Data Link“

Tabelle 103: WBM-Seite „BACnet Status” – Gruppe „BACnet Data Link“

Parameter	Bedeutung
Connection Info	Hier wird der Verbindungsstatus angezeigt.

15.1.1.3.2 Seite „BACnet Configuration“

Auf dieser Seite können Sie für den Feldbus BACnet spezifische Einstellungen vornehmen.

Um eine Einstellung zu übernehmen, klicken Sie die Schaltfläche **[Submit]**.
Die Änderungen in der BACnet Konfiguration werden erst nach einem Neustart übernommen. Nutzen Sie für einen Neustart des Stacks/Controllers die Reboot-Funktion des WBM.

Gruppe „Restart“

Tabelle 104: WBM-Seite „BACnet Configuration ” – Gruppe „BACnet Restart“

Parameter	Bedeutung
Connection Info	Hier wird der Verbindungsstatus angezeigt.

Gruppe „BACnet Service“

Diese Gruppe beinhaltet die Aktivierung und Deaktivierung für den Feldbus.

Der Parameter „Service active“ muss aktiviert sein (Standardeinstellung), damit das Feldbusprotokoll BACnet genutzt werden kann.

Beim Neustart des Laufzeitsstems erfolgt zur Sicherheit eine Abfrage über ein Pop-Up-Fenster, ob der Neustart gewünscht ist.

Tabelle 105: WBM-Seite „BACnet Configuration” – Gruppe „BACnet Service“

Parameter	Bedeutung	
Service active	Hier aktivieren/deaktivieren Sie den Feldbus BACnet.	
Mode	Hier wählen Sie den BACnet Betriebsmodus aus.	
	Ip	Kommunikation über BACnet/IP
	sc	Kommunikation über BACnet/SC
Who-Is online interval time (sec)	Hier stellen Sie ein, in welchen Abständen der Controller Anfragen auf den Feldbus sendet, welche weiteren Teilnehmer online sind (minimal: 60 sec).	
Broadcast I-Am answer	Hier aktivieren/deaktivieren Sie die Möglichkeit, dass die I-Am Nachrichten des Gerätes an die BACnet Broadcast Adresse gesendet werden.	

Gruppe „BACnet Data“

Diese Gruppe bietet die Möglichkeit, auszuwählen, welche Daten beim nächsten Neustart gelöscht oder zurückgesetzt werden sollen.

Tabelle 106: WBM-Seite „BACnet Configuration” – Gruppe „BACnet Data Reset“

Parameter	Bedeutung
Delete Persistence Data	Beim nächsten Neustart werden die persistenten BACnet-Daten gelöscht.
Reset all BACnet Data and Settings to Default	Beim nächsten Neustart werden die BACnet spezifischen Einstellungen und Daten auf Werkseinstellungen zurückgesetzt.
Bereich “override.xml”	
Chose file …	Hier wählen Sie die gewünschte Datei auf dem PC aus.
[Upload]	Mit dieser Schaltfläche übertragen Sie die ausgewählte Datei vom PC zum Controller.

Gruppe „BACnet Log Level“

Tabelle 107: WBM-Seite „BACnet Configuration” – Gruppe „Log Level“

Parameter	Bedeutung
Error	Hier aktivieren/deaktivieren Sie Error-Logausgaben.
Warning	Hier aktivieren/deaktivieren Sie Warning-Logausgaben.
Info	Hier aktivieren/deaktivieren Sie Info-Logausgaben.
Debug	Hier aktivieren/deaktivieren Sie Debug-Logausgaben.

Gruppe „BACnet Network Capture“

Tabelle 108: WBM-Seite „BACnet Configuration” – Gruppe „Network Capture“

Parameter	Bedeutung
Enable	Hier aktivieren/deaktivieren Sie die Aufzeichnung des Netzwerkverkehrs mit den entsprechenden BACnet Filtern.
Log pre-master secrets	Hier aktivieren/deaktivieren Sie die Speicherung der „secrets“ für die Entschlüsselung des BACnet/SC Netzwerkverkehrs.
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.

15.1.1.3.3 Seite „BACnet Data Link“

Auf dieser Seite können Sie die notwendige Einstellung für die gewählte BACnet Betriebsart vornehmen.

Um eine Einstellung zu übernehmen, klicken Sie die Schaltfläche **[Submit]**. Die Änderungen in der BACnet-Konfiguration werden erst nach einem Neustart übernommen. Nutzen Sie für einen Neustart des Stacks/Controllers die Reboot-Funktion des WBM. Um die Laufzeitumgebung neu zu starten, nutzen Sie die Schaltfläche **[Restart]**. Schalten Sie den Controller nicht zu früh aus!

Gruppe „PLC Runtime“

Tabelle 109: WBM-Seite „BACnet Data Link” – Gruppe „PLC Runtime“

Parameter	Bedeutung
[Restart]	Mit dieser Schaltfläche führen sie einen Neustart des BACnet Service durch.

Gruppe „BACnet/IP“

Tabelle 110: WBM-Seite „BACnet Data Link” – Gruppe „BACnet/IP“

Parameter	Bedeutung
Port number	Hier stellen Sie den Port für die BACnet/IP Kommunikation ein.

Gruppe „BACnet/SC“

Tabelle 111: WBM-Seite „BACnet Data Link” – Gruppe „BACnet/SC“

Parameter	Bedeutung	
Mode	Hier wählen sie die BACnet/SC Betriebsart aus.	
	Node	Das Gerät wird als BACnet/SC Node betrieben.
	Primary Hub	Das Gerät wird als BACnet/SC Primary HUB betrieben.
	Failover Hub	Das Gerät wird als BACnet/SC Failover HUB betrieben.
Port number	Hier stellen Sie den Port für die BACnet/SC Kommunikation ein.	
Primary Hub URI	Hier stellen Sie die URI für des Primary HUBs ein. Dabei ist die Eingabe wie folgt aufzubauen: wss://<IP-Adresse>:<Port des HUBs> bzw. wss://<Domain-Name>:<Port des HUBs> (Bsp. wss://192.168.178.19:47808 bzw. wss://PFC200V3-XXXXXX.localdomain.lan:47808)	
Failover Hub URI	Hier stellen Sie die URI für des Failover HUBs ein. Dabei ist die Eingabe wie folgt aufzubauen: wss://<IP-Adresse>:<Port des HUBs> bzw. wss://<Domain-Name>:<Port des HUBs> (Bsp. wss://192.168.178.19:47808 bzw. wss://PFC200V3-XXXXXX.localdomain.lan:47808)	
Allow self signed certificates	Hier aktivieren/deaktivieren Sie, ob die Kommunikation über selbstsignierte Zertifikate aufgebaut werden darf oder nicht.	
Allow expired certificates	Hier aktivieren/deaktivieren die Option, ob eine Verbindung mit abgelaufenen Zertifikaten zugelassen/aufgebaut werden kann oder nicht.	
Accept any certificates	Über diese Option aktivieren/Deaktivieren sie die Möglichkeit, eine Kommunikationsbeziehung mit Teilnehmern ohne korrekte Zertifikate aufzubauen. Durch die Aktivierung dieser Option wird die Kommunikationssicherheit entscheidend vermindert.	

Gruppe „BACnet/SC Certificate Authority (CA)“

Tabelle 112: WBM-Seite „BACnet Data Link” – Gruppe „BACnet/SC Certificate Authority (CA)“

Parameter	Bedeutung
Chose file …	Hier wählen Sie das entsprechende CA-Zertifikat auf Ihrem Computer für die Übertragung auf das Gerät aus.
[Upload]	Mit dieser Schaltfläche übertragen Sie das ausgewählte Zertifikat als CA-Zertifikat auf das Gerät. Nach dem Neustart wird dieses Zertifikat dann als CA-Zertifikat für die BACnet/SC Kommunikation verwendet.

Gruppe „BACnet/SC Certificate“

Tabelle 113: WBM-Seite „BACnet Data Link” – Gruppe „BACnet/SC Certificate“

Parameter	Bedeutung
Chose file …	Hier wählen Sie das entsprechende Gerätezertifikat auf Ihrem Computer für die Übertragung aus.
[Upload]	Mit dieser Schaltfläche übertragen Sie das ausgewählte Geräte Zertifikat auf das Gerät. Nach dem Neustart wird dieses Zertifikat dann für die BACnet/SC Kommunikation verwendet.

Gruppe „BACnet/SC Certificate Signing Request (CSR)“

Für die Erstellung von Geräte Zertifikaten ist die Generierung eines sogenannten „Certificate Signing Request“ (kurz CSR) notwendig. Dieser Request beinhaltet alle notwendigen Informationen für die Zertifizierungsstelle. Mit der Generierung eines neuen CSR wird automatisch ein neuer private Key erzeugt. Somit wird das auf dem Gerät vorhandene Gerätezertifikat unbrauchbar. Die notwendigen Informationen für die Erstellung des CSR werden aus dem aktuell vorhanden Gerätezertifikat ausgelesen.

Tabelle 114: WBM-Seite „BACnet Data Link” – Gruppe „BACnet/SC Certificate Signing Request (CSR)“

Parameter	Bedeutung
[Generate]	Mit Betätigung dieser Schaltfläche wird ein CSR sowie ein neuer privater Schlüssel auf dem Gerät erzeugt.
[Upload]	Mit dieser Schaltfläche lässt sich der erstellte CSR vom Gerät herunterladen.

Gruppe „BACnet/SC Default Certificates“

Das Gerät besitzt die Möglichkeit, Standardzertifikate für die Kommunikation zu verwenden. Da alle WAGO Geräte über diese Möglichkeit verfügen, lässt sich so schnell ein entsprechendes Netzwerk aufbauen. Netzwerke, die mit diesen Zertifikaten arbeiten können, jedoch leicht korrumpiert werden.

Tabelle 115: WBM-Seite „BACnet Data Link” – Gruppe „BACnet/SC Default Certificates“

Parameter	Bedeutung
[Generate]	Mit Betätigung dieser Schaltfläche werden die entsprechenden Default-Zertifikate erstellt

15.1.1.3.4 Seite „BACnet Storage Location“

Auf dieser Seite können Sie Einstellungen für die Speicherung der BACnet spezifischen Parameter vornehmen.

Änderungen werden ohne einen Neustart übernommen.

Gruppe „BACnet Persistence“

Diese Gruppe bietet die Möglichkeit, auszuwählen, auf welchem Speicherort (SD-Card/Internal-Flash) die Persistenzdaten gespeichert werden.

Werden die Persistenzeinstellungen geändert, macht ein Pop-Up-Fenster darauf aufmerksam, dass es zu einem Datenverlust kommen kann, bis die nächste Persistierung vollständig durchgeführt wurde.

Tabelle 116: WBM-Seite „BACnet Storage Location” – Gruppe „BACnet Persistence“

Parameter	Bedeutung	
Storage location	Hier wählen Sie den Speicherort für die Persistenzdaten aus. 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.

Gruppe „BACnet Trendlog”

Diese Gruppe bietet die Möglichkeit, auszuwählen, auf welchem Speicherort (SD-Card/Internal-Flash) die Trendlogdaten gespeichert werden.

Tabelle 117: WBM-Seite „BACnet Storage Location” – Gruppe „BACnet Trendlog“

Parameter	Bedeutung	
Storage location	Hier wählen Sie den Speicherort für die Trendlogdaten aus. 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.

Gruppe „BACnet Eventlog”

Diese Gruppe bietet die Möglichkeit, auszuwählen, auf welchem Speicherort (SD-Card/Internal-Flash) die Event-Log-Daten gespeichert werden.

Tabelle 118: WBM-Seite „BACnet Storage Location” – Gruppe „BACnet Eventlog“

Parameter	Bedeutung	
Storage location	Hier wählen Sie den Speicherort für die Event-Log-Daten aus. 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.

15.1.1.4 Registerkarte „Security“

15.1.1.4.1 Seite „OpenVPN / IPsec Configuration“

Auf der Seite „OpenVPN / IPsec Configuration“ finden Sie die Einstellungen zu OpenVPN und IPsec.

Gruppe „OpenVPN“

Tabelle 119: WBM-Seite „OpenVPN / IPsec Configuration“ – Gruppe „OpenVPN“

Parameter	Bedeutung	
Current State	Hier wird der aktuelle Status des OpenVPN-Dienstes angezeigt.	
	stopped	Der Dienst ist nicht aktiv.
	running	Der Dienst ist aktiv.
OpenVPN enabled	Hier aktivieren oder deaktivieren Sie den OpenVPN-Dienst.	
openvpn.config	Hier wählen Sie eine OpenVPN-Konfigurationsdatei aus, die vom PC zum Produkt oder umgekehrt übertragen werden soll.	

Um eine Änderung zu übernehmen, klicken Sie die Schaltfläche **[Submit]**.

Um eine Datei auf dem PC auszuwählen, klicken Sie das Auswahlfeld **Choose file …**.

Um die ausgewählte Datei vom PC zum Produkt zu übertragen, klicken Sie die Schaltfläche **[Upload]**.

Um eine Datei vom Produkt zum PC zu übertragen, klicken Sie die Schaltfläche **[Download]**.

Die Änderungen werden erst nach dem nächsten Neustart des Produktes wirksam. Nutzen Sie hierzu die Reboot-Funktion des WBM. Schalten Sie das Produkt nicht zu früh aus!

Gruppe „IPsec“

Tabelle 120: WBM-Seite „OpenVPN / IPsec Configuration“ – Gruppe „IPsec“

Parameter	Bedeutung	
Current State	Hier wird der aktuelle Status des IPsec-Dienstes angezeigt.	
	stopped	Der Dienst ist nicht aktiv.
	running	Der Dienst ist aktiv.
IPsec enabled	Hie aktivieren oder deaktivieren Sie den IPsec-Dienst.	
ipsec.conf	Hier wählen Sie eine IPsec-Konfigurationsdatei aus, die vom PC zum Produkt oder umgekehrt übertragen werden soll.	
ipsec.secrets	Hier wählen Sie eine IPsec-Konfigurationsdatei aus, die vom PC zum Produkt übertragen werden soll.	

Um eine Änderung zu übernehmen, klicken Sie die Schaltfläche **[Submit]**.

Um eine Datei auf dem PC auszuwählen, klicken Sie das Auswahlfeld **Choose file …**.

Um die ausgewählte Datei vom PC zum Produkt zu übertragen, klicken Sie die Schaltfläche **[Upload]**.

Um eine Datei vom Produkt zum PC zu übertragen, klicken Sie die Schaltfläche **[Download]**.

Die Änderungen werden erst nach dem nächsten Neustart des Produktes wirksam. Nutzen Sie hierzu die Reboot-Funktion des WBM. Schalten Sie das Produkt nicht zu früh aus!

15.1.1.4.2 Seite „General Firewall Configuration“

Auf der Seite „General Firewall Configuration“ finden Sie die globalen Einstellungen zur Firewall.

Gruppe „Global Firewall Parameter“

Tabelle 121: WBM-Seite „General Firewall Configuration“ – Gruppe „Global Firewall Parameter“

Parameter	Bedeutung
Firewall enabled entirely	Hier aktivieren oder deaktivieren Sie die komplette Funktionalität der Firewall. 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 Sie die Firewall-Parameter korrekt einstellen können, bevor Sie die Firewall aktivieren. 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 <n>“.
ICMP echo broadcast protection	Hier aktivieren oder deaktivieren Sie den „ICMP echo broadcast“-Schutz.
Max. UDP datagrams per second	Hier geben Sie die maximale Anzahl der Datagramme mit gleichen Quellports und gleichen Zielports zwischen Hosts pro Sekunde an.
Max. TCP connections per second	Hier geben Sie die maximale Anzahl der TCP-Verbindungen pro Sekunde an.

Um die Änderung zu übernehmen, klicken Sie die entsprechende Schaltfläche **[Submit]**. Die Änderung wird sofort wirksam.

15.1.1.4.3 Seite „Interface Configuration“

Auf der Seite „Interface Configuration“ finden Sie die Firewall-Einstellungen zu den einzelnen Schnittstellen.

Gruppe „Firewall Configuration Bridge <n> / VPN / WAN“

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

Parameter	Bedeutung
Firewall enabled for Interface	Hier aktivieren oder deaktivieren Sie die Firewall für die jeweilige Bridge.
ICMP echo protection	Hier aktivieren oder deaktivieren Sie den „ICMP echo“-Schutz für die jeweilige Bridge. Wenn Sie den „ICMP echo“-Schutz aktivieren, werden alle „ICMP Echo Requests“ (Pings) abgelehnt und die Eingaben bei „ICMP echo limit per second“ und bei „ICMP burst limit“ sind unwirksam.
ICMP echo limit per second	Hier geben Sie die maximale Anzahl „ICMP pings“ pro Sekunde an. Die Eingabe ist nur bei deaktiviertem „ICMP echo protection“-Schutz wirksam. „0“ = „Disabled“
ICMP burst limit (0 = disabled)	Hier geben Sie die maximale Anzahl „ICMP echo burst“ pro Sekunde an. Die Eingabe ist nur bei deaktiviertem „ICMP echo protection“-Schutz wirksam. „0“ = „Disabled“
Service Configuration	Hier aktivieren oder deaktivieren Sie die Firewall für den jeweiligen Dienst.
FTP/FTPES	Die Dienste selber müssen über die Seite „Ports and Services“ gesondert ein- und ausgeschaltet werden.
FTPS (implicit)	
HTTP	
HTTPS	
I/O-CHECK	
PLC Runtime	
WebVisu – HTTP (port 8080)	
WebVisu – HTTPS (port 8081)	
SSH	
SNMP	
OPC UA (Port 4840)	
BACnet (Port 47808)	
DNP3 (port 20000)	
IEC60870-5-104 (port 2404)	
IEC61850 (port 102)	

Um eine Änderung zu übernehmen, klicken Sie die entsprechende Schaltfläche **[Submit]**. Die Änderung wird sofort wirksam.

15.1.1.4.4 Seite „Configuration of MAC address filter“

Auf der Seite „Configuration of MAC address filter“ 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-Maske:	ff:ff:ff:00:00:00

Beschreibung.	Enable docker bridges
MAC-Adresse:	02:42:00:00:00:00
MAC-Maske:	ff:ff:00:00:00:00

Wenn Sie den ersten Default-Eintrag freischalten, können bereits verschiedene WAGO Geräte 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 Gerät zugreifen. Dies gilt auch für andere Dienste, die von Ihrem Gerät 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 Gerät 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 123: WBM-Seite „Configuration of MAC address filter“ – Gruppe „Global MAC address filter state“

Parameter	Bedeutung
Filter enabled	Hier aktivieren oder deaktivieren Sie den globalen MAC-Adressenfilter.

Um die Änderung zu übernehmen, klicken Sie die Schaltfläche **[Submit]**. Die Änderung wird sofort wirksam.

Gruppe „MAC address filter state Bridge <n>“

Für jede konfigurierte Bridge wird eine eigene Gruppe angezeigt.

Tabelle 124: WBM-Seite „Configuration of MAC address filter“ – Gruppe „MAC address filter state Bridge <n>“

Parameter	Bedeutung
Filter enabled	Hier aktivieren oder deaktivieren Sie den MAC-Adressenfilter für die jeweilige Bridge. Diese Einstellung ist unabhängig von der Einstellung zu „Firewall enabled entirely“ auf der Seite „General Firewall Configuration“.

Um die Änderung zu übernehmen, klicken Sie die Schaltfläche **[Submit]**. Die Änderung wird sofort wirksam.

Gruppe „MAC address filter whitelist“

Für jeden Listeneintrag wird ein eigener Bereich angezeigt.

Tabelle 125: 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	Hier wird die MAC-Adresse des jeweiligen Listeneintrags angezeigt.
MAC mask	Hier wird die MAC-Maske des jeweiligen Listeneintrags angezeigt.
Filter enabled	Hier aktivieren oder deaktivieren Sie den Filter für den jeweiligen Listeneintrag.
Add filter to whitelist	Hier erstellen Sie einen neuen Listeneintrag.
MAC address	Hier geben Sie die MAC-Adresse für einen neuen Listeneintrag ein. Sie können 10 Filter eintragen.
MAC mask	Hier geben Sie die MAC-Maske für den neuen Listeneintrag ein.
Filter enabled	Hier aktivieren oder deaktivieren Sie den Filter für den neuen Listeneintrag.

Um eine Änderung zu übernehmen, klicken Sie die entsprechende Schaltfläche **[Submit]**. Die Änderung wird sofort wirksam.

Um einen bestehenden Listeneintrag zu löschen, klicken Sie die entsprechende Schaltfläche **[Delete]**. Die Änderung wird sofort wirksam.

Um einen neuen Listeneintrag zu übernehmen, klicken Sie die Schaltfläche **[Add]**. Sie können 10 Filter eintragen. Die Änderung wird sofort wirksam.

15.1.1.4.5 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 126: WBM-Seite „Configuration of User Filter“ – Gruppe „User filter“

Parameter	Bedeutung
Policy	Hier wird angezeigt, ob der Netzwerkteilnehmer durch den Filter zugelassen oder ausgeschlossen ist.
Source IP address	Hier wird die Quell-IP-Adresse für den jeweiligen Filter angezeigt.
Source Netmask	Hier wird die Quellnetzmaske für den jeweiligen Filter angezeigt.
Source Port	Hier wird die Quell-Port-Nummer für den jeweiligen Filter angezeigt.
Destination IP address	Hier wird die Ziel-IP-Adresse für den jeweiligen Filter angezeigt.
Destination Netmask	Hier wird die Zielnetzmaske für den jeweiligen Filter angezeigt.
Destination Port	Hier wird die Ziel-Port-Nummer für den jeweiligen Filter angezeigt.
Protocol	Hier werden die zugelassenen Protokolle für den jeweiligen Filter angezeigt.
Input interface	Hier werden die zugelassenen Schnittstellen für den jeweiligen Filter angezeigt.

Tabelle 126: WBM-Seite „Configuration of User Filter“ – Gruppe „User filter“

Parameter	Bedeutung	
Add new user filter	Hier können Sie maximal 10 Filter anlegen. Sie müssen nur Werte in die Felder eintragen, die beim Filter gesetzt werden sollen. Mindestens 1 Wert muss eingetragen werden, alle anderen Felder können leer bleiben.	
Policy	Hier wählen Sie aus, ob der Netzwerkteilnehmer durch den Filter zugelassen oder ausgeschlossen werden soll.	
	Allow	Der Netzwerkteilnehmer ist zugelassen.
	Drop	Der Netzwerkteilnehmer ist ausgeschlossen.
Source IP address	Hier geben Sie die Quell-IP-Adresse für den neuen Filter ein.	
Source netmask	Hier geben Sie die Quellnetzmaske für den neuen Filter ein.	
Source port	Hier geben Sie die Quell-Port-Nummer für den neuen Filter ein.	
Destination IP address	Hier geben Sie die Ziel-IP-Adresse für den neuen Filter ein.	
Destination subnet mask	Hier geben Sie die Zielnetzmaske für den neuen Filter ein.	
Destination port	Hier geben Sie die Ziel-Port-Nummer für den neuen Filter ein.	
Protocol	Hier geben Sie die Protokolle für den neuen Filter ein.	
	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	Hier geben Sie die Schnittstellen für den neuen Filter ein.	
	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.

Um den neuen Filter zu übernehmen, klicken Sie die Schaltfläche **[Add]**. Die Änderung wird sofort wirksam.

Um einen bestehenden Filter zu löschen, klicken Sie die Schaltfläche **[Delete]**. Die Änderung wird sofort wirksam.

15.1.1.4.6 Seite „Certificates“

Auf der Seite „Certificates“ finden Sie Auswahlmöglichkeiten, um Zertifikate und Schlüssel zu installieren oder zu löschen.

Gruppe „Installed Certificates“

Tabelle 127: WBM-Seite „Certificates“ – Gruppe „Certificate List“

Parameter	Bedeutung
<certificate name>	Hier werden die geladenen Zertifikate angezeigt. Wenn kein Zertifikat geladen wurde, wird „No certificates existing“ angezeigt.

Um eine Datei auf dem PC auszuwählen, klicken Sie das Auswahlfeld **Choose file …**.

Um die ausgewählte Datei zum Produkt zu übertragen, klicken Sie die Schaltfläche **[Upload]**. Die Änderungen werden sofort wirksam.

Die Zertifikate werden im Verzeichnis „/etc/certificates/“ und die Schlüssel im Verzeichnis „/etc/certificates/keys/“ gespeichert.

Um einen Eintrag zu löschen, klicken Sie die Schaltfläche **[Delete]**. Die Änderungen werden sofort wirksam.

Gruppe „Installed Private Keys“

Tabelle 128: WBM-Seite „Certificates“ – Gruppe „Private Key List“

Parameter	Bedeutung
<private key name>	Hier werden die geladenen Schlüssel angezeigt. Wenn kein Schlüssel geladen wurde, wird „No private keys existing“ angezeigt.

Um eine Datei auf dem PC auszuwählen, klicken Sie das Auswahlfeld **Choose file …**.

Um die ausgewählte Datei zum Produkt zu übertragen, klicken Sie die Schaltfläche **[Upload]**. Die Änderungen werden sofort wirksam.

Die Zertifikate werden im Verzeichnis „/etc/certificates/“ und die Schlüssel im Verzeichnis „/etc/certificates/keys/“ gespeichert.

Um einen Eintrag zu löschen, klicken Sie die Schaltfläche **[Delete]**. Die Änderungen werden sofort wirksam.

15.1.1.4.7 Seite „Boot mode configuration“

Auf der Seite „Boot mode configuration“ finden Sie Einstellungen zur Boot-Option.

Gruppe „Force internal boot“

Tabelle 129: WBM-Seite „Boot mode configuration” – Gruppe „Force internal boot“

Parameter	Bedeutung	
Boot mode	Hier stellen Sie die Boot-Option für das Produkt ein.	
	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.

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.

Um eine Änderung zu übernehmen, klicken Sie die Schaltfläche **[Submit]**. Die Änderung wird sofort wirksam.

15.1.1.4.8 Seite „Security Settings“

Auf der Seite „Security Settings“ finden Sie Einstellungen zur Netzwerksicherheit.

Gruppe „TLS Configuration“

Tabelle 130: WBM-Seite „Security Settings” – Gruppe „TLS Configuration“

Parameter	Bedeutung	
TLS Configuration	Hier stellen Sie ein, welche TLS-Versionen und kryptografischen Verfahren für HTTPS erlaubt sind.	
	Standard	Der Webserver erlaubt TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3 und auch kryptografische Verfahren, die heute nicht mehr als sicher angesehen werden.
	Strong	Der Webserver erlaubt nur die TLS-Version 1.2, 1.3 und starke Algorithmen. Ältere Software und ältere Betriebssysteme unterstützen eventuell TLS 1.2 und TLS 1.3 nicht.

Um eine Änderung zu übernehmen, klicken Sie die Schaltfläche **[Submit]**. Die Änderung wird sofort wirksam.

Information

Technische Richtlinie TR-02102 des BSI
Die Regeln für die Einstellung „Strong“ richten sich nach der technischen Richtlinie TR-02102 des Bundesamtes für Sicherheit in der Informationstechnik.
Die Richtlinie finden Sie im Internet unter: https://www.bsi.bund.de > „Publikationen“ > „Technische Richtlinien“.

15.1.1.4.9 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 131: WBM-Seite „Advanced Intrusion Detection Environment (AIDE)” – Gruppe „Run AIDE check at startup“

Parameter	Bedeutung
Service active	Hier aktivieren/deaktivieren Sie den „AIDE check“ beim Starten des Controllers.

Um die Änderungen zu übernehmen, klicken Sie die Schaltfläche **[Submit]**. Die Änderungen werden beim nächsten Neustart wirksam.

Gruppe „Refresh Options“

Tabelle 132: WBM-Seite „Advanced Intrusion Detection Environment (AIDE)” – Gruppe „Control AIDE and show log“

Parameter	Bedeutung	
Select Action	Hier wählen Sie die auszuführende Aktion aus.	
	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	Hier schalten Sie die Anzeige der letzten n Meldungen ein. Hier geben Sie zusätzlich die Anzahl der angezeigten Meldungen ein.	
Automatic refresh interval (sec)	Markieren Sie das Kontrollfeld, um die zyklische Aktualisierung einzuschalten. Geben Sie die Zykluszeit in Sekunden ein, mit der eine zyklische Aktualisierung durchgeführt wird. Abhängig von Status wechselt die Beschriftung der Schaltfläche („Refresh“/„Start“/„Stop“).	

Um die Anzeige zu aktualisieren, klicken Sie die Schaltfläche **[Refresh]**. Die Schaltfläche ist nur sichtbar, wenn die zyklische Aktualisierung nicht eingeschaltet ist.

Um die zyklische Aktualisierung zu aktivieren, klicken Sie die Schaltfläche **[Start]**. Die Schaltfläche ist nur sichtbar, wenn die zyklische Aktivierung eingeschaltet ist und noch nicht gestartet wurde.

Um die zyklische Aktualisierung wieder zu beenden, klicken Sie die Schaltfläche **[Stop]**. Diese Schaltfläche ist nur sichtbar, wenn die zyklische Aktualisierung aktiv ist.

Die zyklische Aktualisierung wird nur solange 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.

15.1.1.4.10 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 „WAGO Device Access“-Funktionalität noch im Beta-Status!

Gruppe „Unauthenticated Requests“

Tabelle 133: 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. Zu 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!

Um eine Änderung zu übernehmen, klicken Sie die Schaltfläche **[Submit]**. Die Änderung wird sofort wirksam.

15.1.1.5 Registerkarte „Diagnostic“

15.1.1.5.1 Seite „Log Message Viewer“

Auf der Seite „Log Message Viewer“ finden Sie die Einstellungen zur Anzeige der Diagnosemeldungen.

Gruppe „Refresh Options“

Tabelle 134: WBM-Seite „Log Message Viewer“ – Gruppe „Refresh Options“

Parameter	Bedeutung	
Read only the last	Hier schalten Sie die Anzeige der letzten n Meldungen ein. Hier geben Sie zusätzlich die Anzahl der angezeigten Meldungen ein.	
Automatic refresh interval (sec)	Markieren Sie das Kontrollfeld, um die zyklische Aktualisierung einzuschalten. Geben Sie die Zykluszeit in Sekunden ein, mit der eine zyklische Aktualisierung durchgeführt wird. Abhängig von Status wechselt die Beschriftung der Schaltfläche („Refresh“/„Start“/„Stop“).	
Source	Hier wählen Sie die Quelle der Diagnosemeldungen aus. Die Drop-Down-Liste ist abhängig vom angemeldeten Benutzer.	
	user	Nur Standard-Diagnosemeldungen
	admin	Standard-Diagnosemeldungen und alle Log-Dateien im Ordner `/var/log/*`

Um die Anzeige zu aktualisieren oder die zyklische Aktualisierung zu aktivieren, klicken Sie die Schaltfläche **[Refresh]**. Diese Schaltfläche ist nur sichtbar, wenn die zyklische Aktualisierung nicht eingeschaltet ist.

Um die zyklische Aktualisierung zu aktivieren, klicken Sie die Schaltfläche **[Start]**. Die Schaltfläche ist nur sichtbar, wenn die zyklische Aktivierung eingeschaltet ist und noch nicht gestartet wurde.

Um die zyklische Aktualisierung wieder zu beenden, klicken Sie die Schaltfläche **[Stop]**. Diese Schaltfläche ist nur sichtbar, wenn die zyklische Aktualisierung aktiv ist.

Die zyklische Aktualisierung wird nur solange durchgeführt, wie die Seite „Diagnostic Information“ geöffnet ist. Wenn Sie die WBM-Seite wechseln, wird die Aktualisierung angehalten, bis Sie die Seite „Diagnostic Information“ erneut aufrufen.

Die Meldungen werden unterhalb der Einstellungen angezeigt.

15.1.1.5.2 Seite „Download“

Gruppe „Diagnostic Information“

Um Diagnoseinformationen vom Gerät herunterzuladen, klicken Sie die Schaltfläche **[Download]**.
Anschließend wird eine Archivdatei erstellt, welche die Lognachrichten, die Firmwareversion und eine Liste mit den installierten Paketen beinhaltet. Diese Datei wird im Downloadverzeichnis auf Ihrem Rechner gespeichert.

15.1.1.5.3 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 aktuellen Status der Netzwerkaufzeichnung wird angezeigt.

Gruppe „State“

Tabelle 135: WBM-Seite „Network Capture“ – Gruppe „State“

Parameter	Bedeutung
Current State	Hier wird der aktuelle Status der Netzwerkaufzeichnung angezeigt.
Last Captured Package Count	Hier werden die bereits aufgezeichneten Netzwerkpakete angezeigt.
Last Refresh Time	Hier wird der Zeitpunkt der letzten Aktualisierung von Current State und Last Captured Package Count angezeigt.

Gruppe „Configuration“

Tabelle 136: WBM-Seite „Network Capture“ – Gruppe „Configuration“

Parameter	Bedeutung	
Enable	Hier schalten Sie die Aufzeichnung ein oder aus.	
Rotate Log Files	Hier schalten Sie das rotierende Aufzeichnen ein oder aus. Ist diese Option eingeschaltet, so 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	Hier geben Sie die maximale Dateigröße für die Datenaufzeichnung ein.	
Storage Location	Hier wählen Sie den Speicherort für die aufgezeichneten Daten aus. Eine 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.
Listen On Network Interface	Hier wählen Sie das Netzwerkinterface aus, von welchem der Netzwerkverkehr mitgeschnitten werden soll. Zur Auswahl stehen Ihnen dabei die verfügbaren Netzwerkschnittstellen des Gerätes.	

Um die Änderungen zu übernehmen, klicken Sie die Schaltfläche **[Submit]**. Die Änderungen werden sofort wirksam.

Gruppe „Filter Configuration“

Tabelle 137: WBM-Seite „Network Capture“ – Gruppe „Filter Configuration“

Parameter	Bedeutung
Capture Filter	Hier können Sie Aufzeichnungsfilter angegeben. 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“.

Klicken Sie die Schaltfläche **[Check]**, um den eingegebenen „Capture Filter“ auf Korrektheit zu überprüfen.

Um die Änderungen zu übernehmen, klicken Sie die Schaltfläche **[Submit]**. Die Änderungen werden sofort wirksam.

Gruppe „Log Download“

Tabelle 138: WBM-Seite „Network Capture“ – Gruppe „Log Download“

Parameter	Bedeutung
Select Log File	Hier wählen Sie einen Mitschnitt aus, welcher mit der Schaltfläche **[Download]** heruntergeladen werden kann.

Klicken Sie die Schaltfläche **[Download]**, um den ausgewählten Mitschnitt vom Gerät herunterzuladen.

Klicken Sie die Schaltfläche **[Download All]**, um alle vorhandenen Mitschnitte vom Gerät herunterzuladen.

Abbildungsverzeichnis

Abbildung 1: Ansicht Vorderseite 19
Abbildung 2: Ansicht oben....19
Abbildung 3: Bedruckung (Beispiel)....20
Abbildung 4: Typenschild (Beispiel)....21
Abbildung 5: Anschluss bei DTE-DCE-Verbindung (1:1) 24
Abbildung 6: Anschluss bei DCE-DCE-Verbindung (cross-over) 25
Abbildung 7: RS-485-Busabschluss 25
Abbildung 8: DIO-Anschlüsse X11 (Beispiel)....28
Abbildung 9: Schematisches Schaltbild 33
Abbildung 10: Beispiel Linux®-Passwort 41
Abbildung 11: Startverhalten 46
Abbildung 12: Browserablauf....47
Abbildung 13: „WAGO Ethernet Settings“ – Startbildschirm (Beispiel)....55
Abbildung 14: „WAGO Ethernet Settings“ – Register Netzwerk (Beispiel) 56
Abbildung 15: „Open DHCP, Beispielbild“ 58
Abbildung 16: Authentifizierung eingeben (Beispiel)....61
Abbildung 17: Passworterinnerung....63
Abbildung 18: WBM-Browserfenster (Beispiel)....68
Abbildung 19: WBM-Kopfzeile mit nicht darstellbaren Registerkarten (Beispiel).68
Abbildung 20: WBM-Statuszeile (Beispiel) 69
Abbildung 21: Demontage von der Tragschiene....80

Tabellenverzeichnis

Tabelle 1: Darstellungen der Zahlensysteme 12
Tabelle 2: Schriftkonventionen 12
Tabelle 3: Bedruckung 20
Tabelle 4: Typenschild 20
Tabelle 5: Anschlüsse auf der Vorderseite 22
Tabelle 6: Anschlüsse oben 22
Tabelle 7: Pinbelegung X3 23
Tabelle 8: Funktion der RS-232-Signale bei DTE/DCE....24
Tabelle 9: Pinbelegung X4 26
Tabelle 10: Pinbelegung X5 26
Tabelle 11: Pinbelegung X11 28
Tabelle 12: SYS-LED 31
Tabelle 13: RUN-LED....31
Tabelle 14: CAN-LED....31
Tabelle 15: Stellungen Betriebsartenschalter 32
Tabelle 16: Technische Daten – Gerät 34
Tabelle 17: Technische Daten – Klimatische Umgebungsbedingungen 34
Tabelle 18: Technische Daten – Spannungsversorgung 34
Tabelle 19: Technische Daten – Hardware....35
Tabelle 20: Technische Daten – Kommunikation....35
Tabelle 21: Technische Daten – Schnittstellen 35
Tabelle 22: Technische Daten – Anschlüsse 36
Tabelle 23: WBM-Benutzer 40
Tabelle 24: Linux®-Benutzer 41
Tabelle 25: Voreingestellte IP-Adressierungen der Ethernet-Schnittstellen 54
Tabelle 26: Netzmaske 255.255.255.0 54
Tabelle 27: Benutzereinstellungen im Auslieferungszustand 63
Tabelle 28: Zugriffsrechte für die WBM-Seiten 65
Tabelle 29: CODESYS V3-Prioritäten 72
Tabelle 30: LED-Signalisierung 75
Tabelle 31: Zubehör – Speicherkarten 83
Tabelle 32: Zubehör – Anschlussleitung und Stecker 83
Tabelle 33: WBM-Seite „Device Status“ – Gruppe „Device Details“....84
Tabelle 34: WBM-Seite „Device Status“ – Gruppe „Network TCP/IP Details“ 85
Tabelle 35: WBM-Seite „PLC Runtime Information” – Gruppe „Runtime“ 87
Tabelle 36: WBM-Seite „PLC Runtime Configuration” – Gruppe „General PLC Runtime Configuration“ 93
Tabelle 37: WBM-Seite „PLC Runtime Configuration” – Gruppe „Webserver Configuration“ 94
Tabelle 38: WBM-Seite „TCP/IP Configuration“ – Gruppe „TCP/IP Configuration“ 95
Tabelle 39: WBM-Seite „TCP/IP Configuration“ – Gruppe „DNS Server“ 96
Tabelle 40: WBM-Seite „Ethernet Configuration“ – Gruppe „Bridge Configuration“ 97
Tabelle 41: WBM-Seite „Ethernet Configuration“ – Gruppe „Switch Configuration“ 98
Tabelle 42: WBM-Seite „Ethernet Configuration“ – Gruppe „Dummy Interfaces“ 99

Tabelle 43: WBM-Seite „Ethernet Configuration“ – Gruppe „VLAN Interfaces“ ...99
Tabelle 44: WBM-Seite „Ethernet Configuration“ – Gruppe „Ethernet Interface Configuration“ 100
Tabelle 45: WBM-Seite „Configuration of Host and Domain Name“ – Gruppe „Hostname“ 101
Tabelle 46: WBM-Seite „Configuration of Host and Domain Name“ – Gruppe „Domain Name“....101
Tabelle 47: WBM-Seite „Routing“ – Gruppe „IP Forwarding through multiple interfaces“ 103
Tabelle 48: WBM-Seite „Routing“ – Gruppe „Custom Routes“....104
Tabelle 49: WBM-Seite „Routing“ – Gruppe „IP-Masquerading“ 106
Tabelle 50: WBM-Seite „Routing“ – Gruppe „Port-Forwarding“....107
Tabelle 51: WBM-Seite „Spanning Tree Protocol“– Gruppe „Status“ 108
Tabelle 52: WBM-Seite „Spanning Tree Protocol“– Gruppe „Parameter Settings“ 110
Tabelle 53: WBM-Seite „Clock Settings“ – Gruppe „Timezone and Format“ 112
Tabelle 54: WBM-Seite „Clock Settings“ – Gruppe „UTC Time and Date“ 112
Tabelle 55: WBM-Seite „Clock Settings“ – Gruppe „Local Time and Date“ 113
Tabelle 56: WBM-Seite „Configuration of Serial Interface” – Gruppe „Current Serial Interface Configuration“....114
Tabelle 57: WBM-Seite „Configuration of Serial Interface” – Gruppe „Assign Owner of Serial Interface“ 114
Tabelle 58: WBM-Seite „Configuration of Serial Interface” – Gruppe „Assign Owner of Serial Interface“ 115
Tabelle 59: WBM-Seite „Configuration of Service Interface” – Gruppe „Assign Owner of Service Interface“....116
Tabelle 60: WBM-Seite „Create bootable Image” – Gruppe „Create bootable image from boot device“....117
Tabelle 61: WBM-Seite „Firmware Backup“ – Gruppe „Firmware Backup“ 118
Tabelle 62: WBM-Seite „Firmware Restore“ – Gruppe „Firmware Restore“ 120
Tabelle 63: WBM-Seite „Active System“ – Gruppe „Boot Device“....122
Tabelle 64: WBM-Seite „Active System“ – Gruppe „System <n> (Internal Flash)“ 122
Tabelle 65: WBM-Seite „Mass Storage“ – Gruppe „Devices“....123
Tabelle 66: WBM-Seite „Mass Storage“ – Gruppe „Create new Filesystem on Memory Card“ 123
Tabelle 67: WBM-Seite „Software Uploads“ – Gruppe „Upload new Software“.124
Tabelle 68: WBM-Seite „Configuration of Network Services“ – Gruppe „FTP“ ..125
Tabelle 69: WBM-Seite „Configuration of Network Services“ – Gruppe „FTPES (explicit FTPS)“ 125
Tabelle 70: WBM-Seite „Configuration of Network Services“ – Gruppe „HTTP“126
Tabelle 71: WBM-Seite „Configuration of Network Services“ – Gruppe „HTTPS“ 126
Tabelle 72: WBM-Seite „Configuration of Network Services“ – Gruppe „I/O-*CHECK*“ 126
Tabelle 73: WBM-Seite „Configuration of NTP Client“ – Gruppe „NTP Client Configuration“ 127
Tabelle 74: WBM-Seite „PLC Runtime Services“ – Gruppe „CODESYS V3“ 128
Tabelle 75: WBM-Seite „SSH Server Settings“ – Gruppe „SSH Server“ 129

Tabelle 76: WBM-Seite „DHCP Server Configuration“ – Gruppe „DHCP Configuration Bridge <n>“ 130
Tabelle 77: WBM-Seite „Configuration of DNS Server“ – Gruppe „DNS Server“ 131
Tabelle 78: WBM-Seite „Overview“ – Gruppe „Connection <n>“ 132
Tabelle 79: WBM-Seite „Configuration of Connection <n>“ – Gruppe „Configuration“ 133
Tabelle 80: Anzeige der Auswahl- und Eingabefelder abhängig von der ausgewählten Cloud-Plattform 136
Tabelle 81: Auswahlmöglichkeit des Datenprotokolls abhängig von der ausgewählten Cloud-Plattform 138
Tabelle 82: Anzeige der Auswahl- und Eingabefelder abhängig vom ausgewählten Datenprotokoll 138
Tabelle 83: Auswahlmöglichkeit des Cache-Modes abhängig vom ausgewählten Datenprotokoll 138
Tabelle 84: Anzeige der Eingabefelder abhängig von der ausgewählten Authentifizierung 139
Tabelle 85: WBM-Seite „Configuration of General SNMP Parameters“ – Gruppe „General SNMP Configuration“ 140
Tabelle 86: WBM-Seite „Configuration of SNMP v1/v2c Parameters“ – Gruppe „Communities“ 141
Tabelle 87: WBM-Seite „Configuration of SNMP v1/v2c Parameters“ – Gruppe „Trap Receivers“ 142
Tabelle 88: WBM-Seite „Configuration of SNMP v3 Parameters“ – Gruppe „Users“ 143
Tabelle 89: WBM-Seite „Configuration of SNMP v3 Parameters“ – Gruppe „Trap Receivers“ 145
Tabelle 90: WBM-Seite „Favorites ” – Gruppen „Favorite n“ 148
Tabelle 91: MicroBrowser – Anmeldedaten 148
Tabelle 92: WBM-Seite „Monitoring” – Gruppe „Monitoring“ 150
Tabelle 93: WBM-Seite „Browser Security” – Gruppe „ Browser Security “ 151
Tabelle 94: WBM-Seite „Commisioning Settings“ – Gruppe „Commissioning“ ..152
Tabelle 95: WBM-Seite „Docker Settings“ – Gruppe „Docker Status“ 153
Tabelle 96: WBM-Seite „Screensaver ” – Gruppe „Screensaver Settings“ 156
Tabelle 97: WBM-Seite „Screensaver ” – Gruppe „Screen Care“ 157
Tabelle 98: WBM-Seite „WBM User Configuration” – Gruppe „Change Password“ 158
Tabelle 99: WBM-Seite „OPC UA Configuration“ – Gruppe „OPC UA Server Configuration“ 159
Tabelle 100: WBM-Seite „OPC UA Configuration“ – Gruppe „OPC UA Server Security Settings“ 160
Tabelle 101: WBM-Seite „BACnet Status” – Gruppe „BACnet Information“ 161
Tabelle 102: WBM-Seite „BACnet Status” – Gruppe „BACnet License“ 161
Tabelle 103: WBM-Seite „BACnet Status” – Gruppe „BACnet Data Link“ 161
Tabelle 104: WBM-Seite „BACnet Configuration ” – Gruppe „BACnet Restart“ 162
Tabelle 105: WBM-Seite „BACnet Configuration” – Gruppe „BACnet Service“ .162
Tabelle 106: WBM-Seite „BACnet Configuration” – Gruppe „BACnet Data Reset“ 163
Tabelle 107: WBM-Seite „BACnet Configuration” – Gruppe „Log Level“ 163
Tabelle 108: WBM-Seite „BACnet Configuration” – Gruppe „Network Capture“164

Tabelle 109: WBM-Seite „BACnet Data Link” – Gruppe „PLC Runtime“ 165
Tabelle 110: WBM-Seite „BACnet Data Link” – Gruppe „BACnet/IP“.....165
Tabelle 111: WBM-Seite „BACnet Data Link” – Gruppe „BACnet/SC“ 166
Tabelle 112: WBM-Seite „BACnet Data Link” – Gruppe „BACnet/SC Certificate Authority (CA)“ 167
Tabelle 113: WBM-Seite „BACnet Data Link” – Gruppe „BACnet/SC Certificate“ 167
Tabelle 114: WBM-Seite „BACnet Data Link” – Gruppe „BACnet/SC Certificate Signing Request (CSR)“.....167
Tabelle 115: WBM-Seite „BACnet Data Link” – Gruppe „BACnet/SC Default Certificates“.....168
Tabelle 116: WBM-Seite „BACnet Storage Location” – Gruppe „BACnet Persistence“.....169
Tabelle 117: WBM-Seite „BACnet Storage Location” – Gruppe „BACnet Trendlog“ 170
Tabelle 118: WBM-Seite „BACnet Storage Location” – Gruppe „BACnet Eventlog“.....170
Tabelle 119: WBM-Seite „OpenVPN / IPsec Configuration“ – Gruppe „OpenVPN“ 171
Tabelle 120: WBM-Seite „OpenVPN / IPsec Configuration“ – Gruppe „IPsec“..172
Tabelle 121: WBM-Seite „General Firewall Configuration“ – Gruppe „Global Firewall Parameter“.....173
Tabelle 122: WBM-Seite „Interface Configuration“ – Gruppe „Firewall Configuration Bridge <n> / VPN / WAN“.....175
Tabelle 123: WBM-Seite „Configuration of MAC address filter“ – Gruppe „Global MAC address filter state“.....177
Tabelle 124: WBM-Seite „Configuration of MAC address filter“ – Gruppe „MAC address filter state Bridge <n>“ 177
Tabelle 125: WBM-Seite „Configuration of MAC address filter“ – Gruppe „MAC address filter whitelist“.....178
Tabelle 126: WBM-Seite „Configuration of User Filter“ – Gruppe „User filter“...179
Tabelle 127: WBM-Seite „Certificates“ – Gruppe „Certificate List“ 181
Tabelle 128: WBM-Seite „Certificates“ – Gruppe „Private Key List“.....181
Tabelle 129: WBM-Seite „Boot mode configuration” – Gruppe „Force internal boot“ 182
Tabelle 130: WBM-Seite „Security Settings” – Gruppe „TLS Configuration“ 183
Tabelle 131: WBM-Seite „Advanced Intrusion Detection Environment (AIDE)” – Gruppe „Run AIDE check at startup“.....184
Tabelle 132: WBM-Seite „Advanced Intrusion Detection Environment (AIDE)” – Gruppe „Control AIDE and show log“.....184
Tabelle 133: WBM-Seite „WAGO Device Access” – Gruppe „Unauthenticated Requests“ 186
Tabelle 134: WBM-Seite „Log Message Viewer“ – Gruppe „Refresh Options“..187
Tabelle 135: WBM-Seite „Network Capture“ – Gruppe „State“ 189
Tabelle 136: WBM-Seite „Network Capture“ – Gruppe „Configuration“.....190
Tabelle 137: WBM-Seite „Network Capture“ – Gruppe „Filter Configuration“....191
Tabelle 138: WBM-Seite „Network Capture“ – Gruppe „Log Download“ 191

WAGO GmbH & Co. KG
Postfach 2880 • 32385 Minden
Hansastraße 27 • 32423 Minden
Telefon: 0571/887 – 0
Telefax: 0571/887 – 844169
E-Mail: info@wago.com
Internet: www.wago.com