WAGO TECHDOCS

Handbuch

# WAGO I/O System Compact

# 751-9301

## Compact Controller 100

**Version 1.6.0, gültig ab FW-Version 04.04.xx(26)**

**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

# Inhaltsverzeichnis

# 1 Hinweise zu dieser Dokumentation

**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 den Controller „Compact Controller 100“ (751-9301).

## 1.2 Urheberschutz

## 1.3 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.

## 1.4 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).

## 1.5 Darstellung der Zahlensysteme

Tabelle 1: Darstellungen der Zahlensysteme

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

## 1.6 Schriftkonventionen

Tabelle 2: Schriftkonventionen

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

# 2 Wichtige Erläuterungen

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.

## 2.1 Rechtliche Grundlagen

### 2.1.1 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.

### 2.1.2 Personalqualifikation

Sämtliche Arbeitsschritte, die an den Geräten des WAGO I/O Systems Compact 751 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.

### 2.1.3 Bestimmungsgemäße Verwendung

Controller des modularen WAGO I/O Systems Compact 751 dienen dazu, digitale und analoge Signale von Sensoren aufzunehmen und an Aktoren auszugeben oder an übergeordnete Steuerungen weiterzuleiten. Mit den Controllern ist zudem eine (Vor-)Verarbeitung möglich.

Das Produkt genügt der Schutzart IP20 und ist für den Einsatz in trockenen Innenräumen ausgelegt. Es besteht Fingerschutz und Schutz gegen feste Fremdkörper ≥ 12,5 mm, jedoch kein Schutz gegen Wasser. Das Produkt stellt ein offenes Betriebsmittel dar. Es darf nur in Umhüllungen (werkzeuggesicherten Gehäusen oder Betriebsräumen) errichtet werden, die die im Kapitel „Sicherheitshinweise“ aufgeführten Anforderungen erfüllen.
Ein Einsatz ohne Schutzmaßnahmen in einer Umgebung, in der Feuchtigkeit, Staub, ätzende Dämpfe, Gase oder ionisierende Strahlung auftreten können, gilt als sachwidrige Verwendung.

Das Produkt ist für den Einbau in Anlagen der Automatisierungstechnik vorgesehen. Es verfügt nicht über eine eigene integrierte Trennvorrichtung. Eine geeignete Trennvorrichtung muss daher anlagenseitig geschaffen werden.

Der Betrieb des Produkts im Wohnbereich ist ohne weitere Maßnahmen nur zulässig, wenn dieses die Emissionsgrenzen (Störaussendungen) gemäß EN 61000-6-3 einhält.
Entsprechende Angaben finden Sie im Kapitel „Gerätebeschreibung“ > „Normen und Richtlinien“ im Handbuch zum eingesetzten Produkt.

### 2.1.4 Technischer Zustand der Geräte

Die Geräte werden ab Werk für den jeweiligen Anwendungsfall mit einer festen Hard- und Softwarekonfiguration ausgeliefert. Sie enthalten keine durch den Anwender zu wartenden oder zu reparierenden Teile. Folgende Handlungen bewirken den Haftungsausschluss der WAGO GmbH & Co. KG:

- Reparaturen,
- Veränderungen an der Hard- oder Software, die nicht in der Bedienungsanleitung beschrieben sind,
- nicht bestimmungsgemäßer Gebrauch der Komponenten.

Weitere Einzelheiten ergeben sich aus den vertraglichen Vereinbarungen. Wünsche an eine abgewandelte bzw. neue Hard- oder Softwarekonfiguration richten Sie bitte an die WAGO GmbH & Co. KG.

## 2.2 Sicherheitshinweise

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

**GEFAHR**

**Nicht an Geräten unter Spannung arbeiten!**
Schalten Sie immer alle verwendeten Spannungsversorgungen für das Gerät ab, bevor Sie es montieren, Störungen beheben oder Wartungsarbeiten vornehmen.

**GEFAHR**

**Produkt in ein geeignetes Gehäuse einbauen!**
Das Produkt ist ein offenes Betriebsmittel. Montieren Sie das Produkt in ein geeignetes Gehäuse. Dieses Gehäuse muss:

- gewährleisten, dass der maximal zulässige Verschmutzungsgrad nicht überschritten wird.
- einen ausreichenden Schutz gegen Berühren bieten.
- einen ausreichenden Schutz gegen UV-Einstrahlung bieten.
- die Ausbreitung von Feuer nach außerhalb des Gehäuses verhindern.
- die Festigkeit gegen mechanische Beanspruchung gewährleisten.
- den Zugang auf autorisiertes Fachpersonal einschränken und darf nur mit Werkzeug zu öffnen sein.

**GEFAHR**

**Trennvorrichtung und Überstromschutz gewährleisten!**
Das Gerät ist für den Einbau in Anlagen der Automatisierungstechnik vorgesehen. Es verfügt nicht über eine integrierte Trennvorrichtung. Angeschlossene Anlagen müssen abgesichert werden.
Sehen Sie anlagenseitig eine geeignete Trennvorrichtung und einen geeigneten Überstromschutz vor.

**GEFAHR**

**Unfallverhütungsvorschriften beachten!**
Beachten Sie bei Montage, Inbetriebnahme, Betrieb, Wartung und Störbehebung die für Ihre Maschine/Anlage zutreffenden Unfallverhütungs-vorschriften 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.

**WARNUNG**

**Speisung ausschließlich aus SELV-/PELV-Versorgung!**
Alle Feldsignale und alle Feldversorgungen, die an den Controller „Compact Controller 100“ (751-9301) angeschlossen werden, müssen aus SELV-/PELV-Versorgung(en) gespeist werden!

**ACHTUNG**

**Einwandfreie Kontaktierung zur Tragschiene gewährleisten!**
Der einwandfreie, elektrische Kontakt zwischen Tragschiene und Gerät ist notwendig, um die EMV-Eigenschaften und Funktion des Gerätes aufrechtzuerhalten.

**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**

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

**ACHTUNG**

**Verpolungen vermeiden!**
Vermeiden Sie die Verpolung der Daten- und Versorgungsleitungen, da dies zu Schäden an den Geräten führen kann.

**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).

**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.

## 2.3 Lizenzbedingungen der eingesetzten Softwarepakete

Die Firmware des Controllers „Compact Controller 100“ (751-9301) enthält Open-Source-Software.

Die Lizenzbedingungen der Softwarepakete sind in Textform im Controller gespeichert. Sie sind über die WBM-Seite „Legal Information“ > „Open Source Software“ aufrufbar.
Den Quellcode mit den Lizenzbedingungen der Open-Source-Software erhalten Sie auf Wunsch von WAGO GmbH & Co. KG. Senden Sie Ihre Anforderung an support@wago.com mit dem Betreff „Controller Board Support Package“.

## 2.4 Spezielle Einsatzbestimmungen für ETHERNET-Geräte

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 direkt 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 WAGO-I/O-CHECK und 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.

- Ist ein Fernzugriff auf Steuerungskomponenten und Steuerungsnetzwerke erforderlich, sollte ein „Virtual Private Network“ (VPN) genutzt werden.

- 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.

- 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

Bei dem Controller „Compact Controller 100“ (751-9301) handelt es sich um ein Automatisierungsgerät, das die Steuerungsaufgaben einer SPS/PLC erledigen kann.
Der Controller ist zur Montage auf einer Hutschiene geeignet und zeichnet sich durch verschiedene Schnittstellen aus. Unter anderem verfügt der Controller über integrierte digitale und analoge Ein- und Ausgänge und eine serielle Onboard-Schnittstelle gemäß EIA-485/RS-485.

Dieser Controller kann für Anwendungen im Maschinen- und Anlagenbau sowie in der Prozessindustrie, der Gebäude- und Energietechnik eingesetzt werden.

Automatisierungsaufgaben lassen sich in allen IEC-61131-3-kompatiblen Sprachen mit dem Programmiersystem CODESYS V3 realisieren.
Die Implementierung der Task-Abarbeitung im Laufzeitsystem ist für Linux® mit Echtzeiterweiterungen optimiert, um die maximale Leistung für Automatisierungsaufgaben bereitzustellen. Zur Visualisierung steht neben der Entwicklungsumgebung auch die Webvisualisierung zur Verfügung.

Für die IEC-61131-3-Programmierung in CODESYS Applikationen stellt der Controller 32 MByte Programmspeicher (Flash) und 128 MByte Datenspeicher (RAM) und 128 kByte Remanent-Speicher (Retain- und Merkervariablen in einem integrierten NVRAM) zur Verfügung.

Zwei ETHERNET-Schnittstellen und der integrierte, konfigurierbare Switch ermöglichen die Verdrahtung in allen notwendigen Konfigurationen mit einem gemeinsamen Netzwerk mit einer gemeinsamen IP-Adresse für beide Schnittstellen oder mit zwei getrennten Netzwerken mit einer eigenen IP-Adresse für jede Schnittstelle.

Die Zuordnung der physikalischen Schnittstellen (Ports) erfolgt dabei über logische Bridges und kann z. B. über das WBM konfiguriert werden.

Beide Schnittstellen unterstützen:

- 10BASE-T / 100BASE-TX
- Voll-/Halbduplex
- Autonegotiation
- Auto-MDI(X) (automatische Uplink- bzw. Crossover-Umschaltung)

Für den Prozessdatenaustausch sind folgende Feldbusanschaltungen implementiert:

- Modbus TCP Client/Server
- Modbus RTU Master/Slave (über RS-485)

- Gateway Modbus TCP zu Modbus RTU
- EtherCAT Master
- EtherNet/IP-Adapter
- EtherNet/IP-Scanner
- OPC UA

Die Feldbuskonfiguration ist mit CODESYS V3 möglich.

Zur Konfiguration steht ihnen weiterhin das Web-Based-Management (WBM) zur Verfügung. Es umfasst verschiedene dynamische HTML-Seiten, über die unter anderem Informationen über die Konfiguration und den Status des Controllers abgerufen werden können. Das WBM ist bereits im Gerät gespeichert und wird über einen Webbrowser dargestellt und bedient. Darüber hinaus können sie im implementierten Dateisystem eigene HTML-Seiten hinterlegen oder Programme direkt aufrufen.

Die im Auslieferungszustand installierte Firmware basiert auf Linux mit speziellen Echtzeiterweiterungen des RT-Preempt-Patches. Zudem sind neben verschiedenen Hilfsprogrammen folgende Anwenderprogramme auf dem Controller installiert:

- ein SNMP-Server/Client
- ein FTP-Server, ein FTPS-Server (nur explizite Verbindungen)
- ein SSH-Server/-Client
- ein Webserver
- ein NTP-Client
- ein BootP- und DHCP-Client
- die CODESYS V3-Laufzeitumgebung

Entsprechend der IEC-61131-3-Programmierung erfolgt die Bearbeitung der Prozessdaten vor Ort im Controller. Die daraus erzeugten Verknüpfungsergebnisse können direkt an die Aktoren ausgegeben oder über einen angeschlossenen Feldbus an die übergeordnete Steuerung übertragen werden.

**Hinweis**

**Speicherkarte ist nicht im Lieferumfang enthalten!**
Beachten Sie, der Controller wird ohne Speicherkarte ausgeliefert.
Für die Nutzung einer Speicherkarte müssen Sie diese separat dazu bestellen.
Der Controller kann auch ohne Speicherkartenerweiterung betrieben werden, die Verwendung einer Speicherkarte ist optional.

**Hinweis**

**Nur empfohlene Speicherkarte verwenden!**
Setzen Sie ausschließlich die von WAGO erhältliche und für den Controller vorgesehene Speicherkarte ein, da diese für industrielle Anwendungen unter erschwerten Umgebungsbedingungen und für den Einsatz in diesem Gerät spezifiziert ist.
Die Kompatibilität zu anderen im Handel erhältlichen Speichermedien kann nicht gewährleistet werden.

# 4 Eigenschaften

## 4.1 Aufbau der Hardware

### 4.1.1 Ansicht

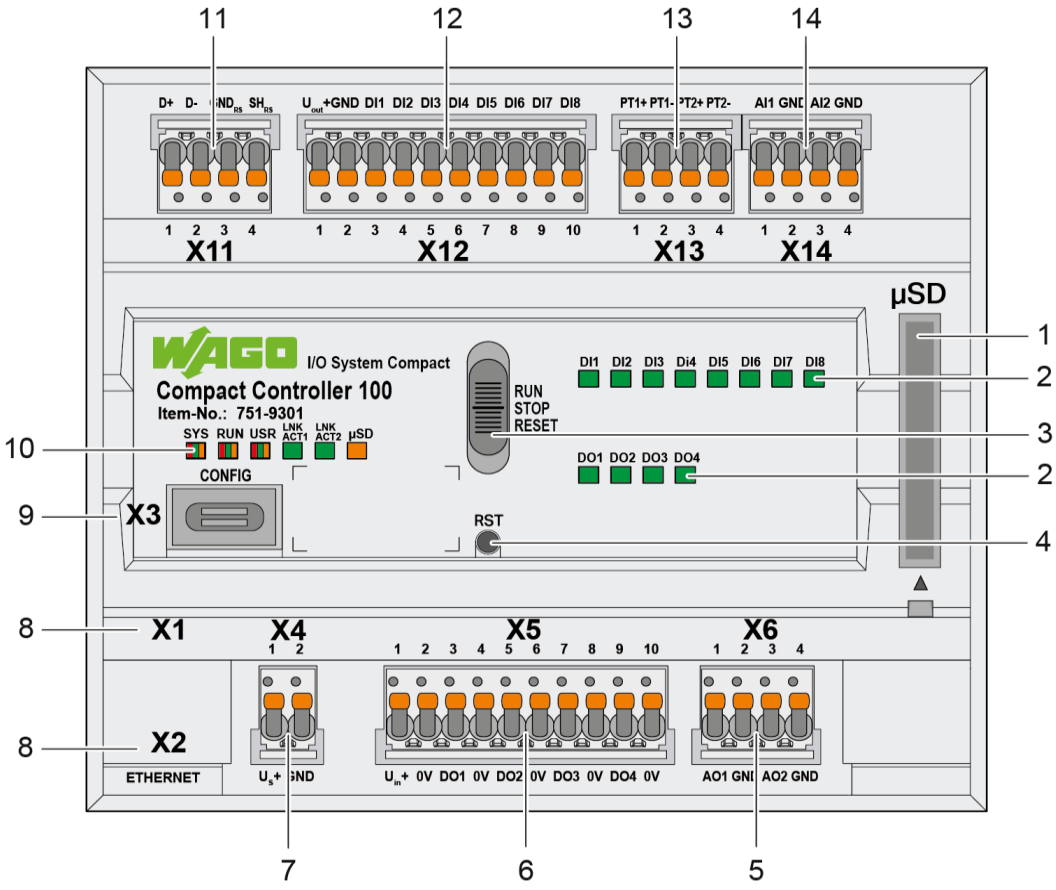



Abbildung 1: Ansicht

Tabelle 3: Legende zur Abbildung „Ansicht“

| Position | Beschreibung | Siehe Kapitel |
|---|---|---|
| 1 | Speicherkartensteckplatz | „Speicherkartensteckplatz“ |
| 2 | LED-Anzeigen – Status DI/DO | „Anzeigeelemente“ > „LEDs Status DI/DO“ |
| 3 | Betriebsartenschalter | „Bedienelemente“ > „Betriebsartenschalter“ |
| 4 | Reset-Taster | „Bedienelemente“ > „Reset-Taster“ |
| 5 | Analoge Ausgänge AO – „X6“ | „Anschlüsse“ > „Analoge Ein- und Ausgänge“ |
| 6 | Digitale Ausgänge DO – „X5“ | „Anschlüsse“ > „Digitale Ein- und Ausgänge“ |
| 7 | Versorgungsspannung System – X4 | „Anschlüsse“ > „Versorgungsspannung“ |
| 8 | Netzwerkanschlüsse ETHERNET – „X1“, „X2“ | „Anschlüsse“ > „Netzwerkanschlüsse“ |
| 9 | Service-Schnittstelle – „X3“ | „Anschlüsse“ > „Service-Schnittstelle“ |
| 10 | LED-Anzeigen – System / Netzwerkanschlüsse / Speicherkartensteckplatz | „Anzeigeelemente“ > „LEDs System“, „Anzeigeelemente“ > „LED Netzwerkanschluss“, „Anzeigeelemente“ > „LED Speicherkartensteckplatz“ |
| 11 | Kommunikationsschnittstelle RS-485 – „X11“ | „Anschlüsse“ > „Kommunikationsschnittstelle“ |
| 12 | Digitale Eingänge DI – „X12“ | „Anschlüsse“ > „Digitale Ein- und Ausgänge“ |
| 13 | Analoge Temperatursensoren – „X13“ | „Anschlüsse“ > „Analoge Temperatursensoren“ |
| 14 | Analoge Eingänge AI – „X14“ | „Anschlüsse“ > „Analoge Ein- und Ausgänge“ |

## 4.1.2 Bedruckung und Typenschild

Die Bedruckung und das Typenschild befinden sich auf der linken Seite des Produkts. Folgende Angaben zum Produkt sind darin enthalten:

Tabelle 4: Bedruckung und Typenschild

| Feld | Beispiel |
|---|---|
| Artikelbezeichnung | Compact Controller 100 |
| Serie | I/O System Compact |
| Bestellnummer | Item-No.: 751-9301 |
| QR-Code | |
| Versorgungsspannung System | 20.4 V ≤ $U_s$ + ≤ 28.8 V / max. 0.5 A |
| Versorgungsspannung Feld (Digitale Ausgänge) | 20.4 V ≤ $U_{in}$ + ≤ 28.8 V / max. 2 A |
| Stromaufnahme Systemversorgung | 20.4 V ≤ $U_{out}$ + ≤ 28.8 V / max. 0.2 A |
| Umgebungstemperatur (Betrieb) | −25 °C ≤ $T_{amb}$ ≤ + 60 °C |
| Seriennummer | UN31564010260470190+ 0000000002342273 |
| Kontrollnummer | 21110.5003 |
| Fertigungsdatum (Jahr – Monat) und Hardware-Revisionsnummer | 2021-09-14 |
| DataMatrix-Code | |
| Barcode (Strichcode) | |

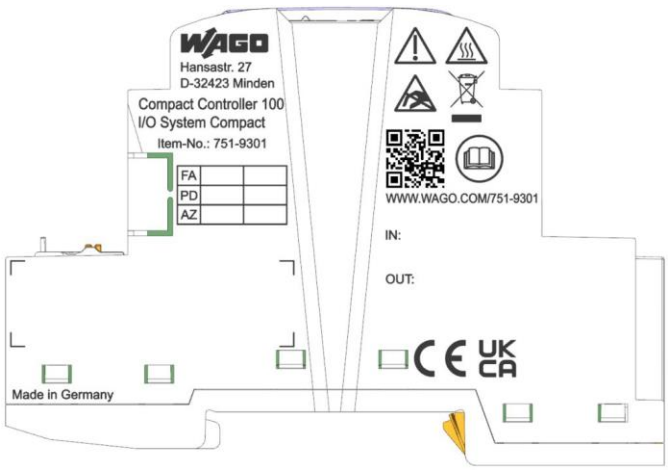



Abbildung 2: Bedruckung (Beispiel)

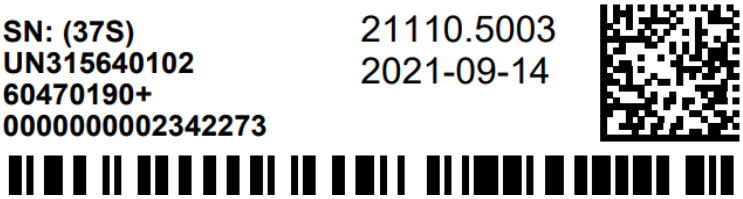



Abbildung 3: Typenschild (Beispiel)

## 4.1.3 Anschlüsse

### 4.1.3.1 Netzwerkanschlüsse

Tabelle 5: Netzwerkanschlüsse ETHERNET– „X1“, „X2“

| Kontakt | Signal | Beschreibung |
|---|---|---|
| 1 | TD+ | Transmit Data + |
| 2 | TD- | Transmit Data - |
| 3 | RD+ | Receive Data + |
| 4 | NC | Nicht belegt |
| 5 | NC | Nicht belegt |
| 6 | RD- | Receive Data - |
| 7 | NC | Nicht belegt |
| 8 | NC | Nicht belegt |

### 4.1.3.2 Service-Schnittstelle

Die Service-Schnittstelle „X3“ wird für die Kommunikation mit WAGO Ethernet-Settings verwendet.

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.

### 4.1.3.3 Versorgungsspannung

Tabelle 6: Versorgungspannung – „X4“

| Kontakt | Signal | Beschreibung |
|---|---|---|
| 1 | $U_S$+ | Versorgungsspannung |
| 2 | GND | Masse |

### 4.1.3.4 Digitale Ein- und Ausgänge

Die Anschlüsse dienen zum Anschluss von Aktoren und Sensoren.
Es werden *picoMAX*®-Steckverbinder mit Push-in CAGE CLAMP®S-Anschlüssen verwendet.

#### 4.1.3.4.1 Digitale Eingänge

Der Controller erfasst binäre Steuersignale aus dem Feldbereich (z. B. von Sensoren, Gebern, Schaltern oder Näherungsschaltern).

Das Produkt besitzt 8 Eingangskanäle (8DI, DC 24 V, 2,8 mA).

Jeder Eingangskanal besitzt zur Störunterdrückung einen RC-Filter mit einer Zeitkonstanten von 5,0 µs.

Die Eingänge sind positivschaltend. Wenn das 24 V-Potential für die Systemversorgung $U_{out}$+ (Klemme „X12“) auf einen Eingangsanschluss geschaltet ist, wird der Signalzustand des entsprechenden Eingangskanals „high“.

Eine grüne Status-LED je Kanal zeigt den Signalzustand an.
Die Bedeutung der LEDs ist im Kapitel „Anzeigeelemente“ > „LEDs Status DI/DO“ beschrieben.

Tabelle 7: Digitale Eingänge – „X12“

| Kontakt | Signal | Beschreibung |
|---|---|---|
| 1 | $U_{out}$+ | Versorgungsspannungsausgang (DI1 … DI8) |
| 2 | GND | Masse |
| 3 | DI1 | Digitaler Eingang 1 |
| 4 | DI2 | Digitaler Eingang 2 |
| 5 | DI3 | Digitaler Eingang 3 |
| 6 | DI4 | Digitaler Eingang 4 |
| 7 | DI5 | Digitaler Eingang 5 |
| 8 | DI6 | Digitaler Eingang 6 |
| 9 | DI7 | Digitaler Eingang 7 |
| 10 | DI8 | Digitaler Eingang 8 |

**Hinweis**

**Potential beachten!**
Der Versorgungsspannungsausgang $U_{out}$+/GND ist nicht kurzschlussfest.

#### 4.1.3.4.2 Digitale Ausgänge

Der Controller gibt binäre Steuersignale aus dem Automatisierungsgerät an die angeschlossenen Aktoren (z. B. Magnetventil, Schütze, Geber, Relais oder andere elektrische Lasten) aus.

Das Produkt besitzt 4 Ausgangskanäle (4DO, 24 V DC 0,5 A).

Die Ausgänge sind positivschaltend. Wenn der Signalzustand eines Ausgangskanals „high“ ist, wird das 24 V-Potential für die Feldversorgung auf den entsprechenden Ausgangskanal geschaltet.

Die Feldversorgung dient der Versorgung der Digitalen Ausgänge.

Eine grüne Status-LED je Kanal zeigt den Signalzustand an.
Die Bedeutung der LEDs ist im Kapitel „Anzeigeelemente“ > „LEDs Status DI/DO“ beschrieben.

Die Feldebene der Digitalen Ausgänge ist von der Systemebene voneinander galvanisch getrennt.

Die Anschlüsse sind gemäß EN 61010-2-201 spezifiziert:
Gleichstromkreis, allgemeine Verwendung

Tabelle 8: Digitale Ausgänge – „X5“

| Kontakt | Signal | Beschreibung |
|---|---|---|
| 1 | $U_{in}$+ | Versorgungsspannungseingang (DO1 … DO4) |
| 2 | 0V | Masse |
| 3 | DO1 | Digitaler Ausgang 1 |
| 4 | 0V | Masse |
| 5 | DO2 | Digitaler Ausgang 2 |
| 6 | 0V | Masse |
| 7 | DO3 | Digitaler Ausgang 3 |
| 8 | 0V | Masse |
| 9 | DO4 | Digitaler Ausgang 4 |
| 10 | 0V | Masse |

#### 4.1.3.5 Analoge Ein- und Ausgänge

Die Anschlüsse dienen zum Anschluss von Aktoren und Sensoren.
Es werden *picoMAX*®-Steckverbinder mit Push-in CAGE CLAMP®S-Anschlüssen verwendet.

##### 4.1.3.5.1 Analoge Eingänge

Der Controller verarbeitet Signale der normierten Größe 0 … +10 V aus dem Feldbereich.

Das Produkt besitzt 2 Eingangskanäle für Feldsignale.

Die Sensoren werden an AI1 und Masse bzw. AI2 und jeweils Masse angeschlossen.

Die Masseanschlüsse liegen für alle 2 Kanäle auf einem gemeinsamen 0 V-Massepotential.

Das Eingangssignal wird mit einer Auflösung von 16 Bit übertragen.

Zur Spannungsversorgung wird die interne Systemspannung genutzt.

Tabelle 9: Analoge Eingänge – „X14“

| Kontakt | Signal | Beschreibung |
|---|---|---|
| 1 | AI1 | Analoger Eingang 1 |
| 2 | GND | Masse |
| 3 | AI2 | Analoger Eingang 2 |
| 4 | GND | Masse |

#### 4.1.3.5.2 Analoge Ausgänge

Der Controller erzeugt Signale der normierten Größe 0 …+10 V für den Feldbereich.

Das Produkt besitzt 2 Ausgangskanäle und ermöglicht die direkte Verdrahtung von zwei 2-Leiter-Aktoren.

Die Aktoren werden über die Anschlüsse AO1 und Masse bzw. AO2 und jeweils Masse angeschlossen.

Die Kanäle besitzen ein gemeinsames Massepotential.

Das Ausgangssignal wird mit einer Auflösung von 12 Bit ausgegeben.

Zur Spannungsversorgung wird die interne Systemspannung genutzt.

Tabelle 10: Analoge Ausgänge – „X6“

| Kontakt | Signal | Beschreibung |
|---|---|---|
| 1 | AO1 | Analoger Ausgang 1 |
| 2 | GND | Masse |
| 3 | AO2 | Analoger Ausgang 2 |
| 4 | GND | Masse |

### 4.1.3.6 Kommunikationsschnittstelle

Die im Controller integrierte Kommunikationsschnittstelle ermöglicht den Anschluss von Geräten mit einer RS-485-Schnittstelle.

Die Verdrahtung zum Kommunikationspartner erfolgt über die Anschlüsse D+, D-, $GND_{RS}$ und $SH_{RS}$.

Der Schirmanschluss ist direkt zur Tragschiene geführt.

Die Schnittstelle arbeitet normenkonform gemäß DIN 66259.

Das angeschlossene Gerät kann über den eingesetzten Controller direkt kommunizieren. Der aktive Kommunikationskanal arbeitet unabhängig vom überlagerten Bussystem im Halbduplexbetrieb mit bis zu 115200 Baud.

Die RS-485-Schnittstelle garantiert eine hohe Störsicherheit durch eine differenzielle Übertragung und galvanisch getrennte Signale.

Tabelle 11: Kommunikationsschnittstelle RS-485 – „X11“

| Kontakt | Signal | Beschreibung |
|---|---|---|
| 1 | D+ | Transmit/receive data + |
| 2 | D– | Transmit/receive data – |
| 3 | $GND_{RS}$ | Masse |
| 4 | $SH_{RS}$ | Schirm |

#### 4.1.3.6.1 Betrieb als RS-485-Schnittstelle

Um Reflektionen am Leitungsende zu minimieren, muss die RS-485-Leitung am Ende mit einem Leitungsabschluss von 120 Ohm terminiert werden. Die RS485-Leitung ist im Compact Controller 100 bereits mit einem Busabschlusswiderstand (120 Ohm) terminiert. Ebenfalls ist im Compact Controller 100 bereits ein Bias-Netzwerk (Pull-up und Pull-down Widerstand) integriert, um die Bus-Leitungen auf einem definierten Pegel zu halten, wenn kein anderer Teilnehmer aktiv ist.

**Hinweis**

**Busabschluss beachten!**
Der RS-485-Bus muss am Ende 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.

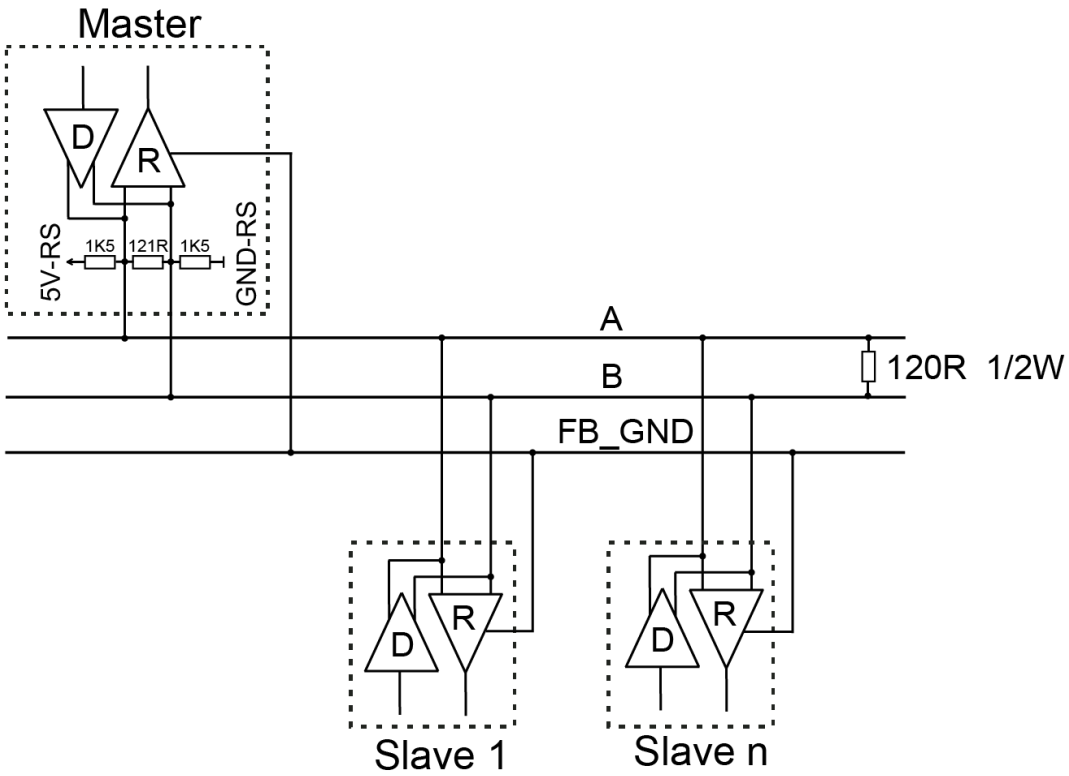



Abbildung 4: RS-485-Busabschluss

### 4.1.3.7 Analoge Temperatursensoren

Die Anschlüsse dienen zum Anschluss von Aktoren und Sensoren.
Es werden *picoMAX*®-Steckverbinder mit Push-in CAGE CLAMP®S-Anschlüssen verwendet.

An den Controller können analoge Temperatursensoren wie Pt1000 oder Ni1000 angeschlossen werden.

Die Widerstandswerte werden in Temperaturwerte umgerechnet. Der Microprozessor linearisiert die gemessenen Widerstandswerte und rechnet sie in einen zur Temperatur des ausgewählten Widerstandssensors proportionalen Zahlenwert um.

Der Controller besitzt 2 Eingangskanäle und ermöglicht den direkten Anschluss von Widerstandssensoren in 2-Leiter-Technik.

Tabelle 12: Analoge Temperatursensoren – „X13“

| Kontakt | Signal | Beschreibung |
|---|---|---|
| 1 | PT1+ | Analoger Eingang Pt1000/Ni1000 |
| 2 | PT1– | |
| 3 | PT2+ | |
| 4 | PT2– | |

## 4.1.4 Anzeigeelemente

### 4.1.4.1 LEDs System

Tabelle 13: LEDs System

| Bezeichnung | Farbe | Beschreibung |
|---|---|---|
| SYS | Rot/Grün/Aus | Systemstatus |
| RUN | Rot/Grün/Aus | PLC-Programmstatus |
| USR | Rot/Grün/Aus | User-LED, programmierbar über Funktionsbausteine der WAGO Bibliotheken zur Ansteuerung der LEDs |

### 4.1.4.2 LED Netzwerkanschluss

Tabelle 14: LEDs „LNK ACT“

| Bezeichnung | Farbe | Beschreibung |
|---|---|---|
| LNK ACT1<br>LNK ACT2 | Grün/Aus | ETHERNET-Verbindungsstatus/ -Datenaustausch |

### 4.1.4.3 LED Speicherkartensteckplatz

Tabelle 15: LED Speicherkartensteckplatz

| Bezeichnung | Farbe | Beschreibung |
|---|---|---|
| µSD | Orange/Aus | Speicherkartenstatus |

### 4.1.4.4 LEDs Status DI/DO

Tabelle 16: LEDs Status DI/DO

| Bezeichnung | Farbe | Beschreibung |
|---|---|---|
| DI1 … DI8<br>DO1 … DO4 | Grün/Aus | Status Digitale Ein- und Ausgänge |

## 4.1.5 Bedienelemente

### 4.1.5.1 Betriebsartenschalter

Tabelle 17: Betriebsartenschalter

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

In Verbindung mit dem Reset-Taster können weitere Funktionen ausgelöst werden.

### 4.1.5.2 Reset-Taster

Der Reset-Taster 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).
Er ist mit einem geeigneten Gegenstand (z. B. einem Kugelschreiber) bedienbar.

Mit dem Reset-Taster können Sie abhängig von der Position des Betriebsartenschalters unterschiedliche Funktionen ausführen:

- Temporär feste IP-Adressen einstellen („Fixed IP Address“-Modus, siehe Kapitel „In Betrieb nehmen“ > „Einstellen einer IP-Adresse“ > „Temporär feste IP-Adressen einstellen“)
- Einen Software-Reset (Neustart) durchführen (siehe Kapitel „In Betrieb nehmen“ > „Reset-Funktionen auslösen“ > „Software-Reset (Neustart)“)
- Einstellungen zurücksetzen (Controller-Reset, siehe Kapitel „In Betrieb nehmen“ > „Reset-Funktionen auslösen“ > „Controller-Reset“)

### 4.1.6 Speicherkartensteckplatz

Der Steckplatz für die SD-Speicherkarte befindet sich auf der Frontseite des Gehäuses. Die Speicherkarte wird mit einem Push/Push-Mechanismus im Gehäuse verriegelt. Das Stecken und Ziehen der Speicherkarte ist im Kapitel „Service“ > „Speicherkarte einfügen und entfernen“ beschrieben!
Die Speicherkarte ist durch eine Abdeckklappe geschützt. Die Abdeckklappe ist plombierbar.

**Hinweis**

**Speicherkarte ist nicht im Lieferumfang enthalten!**
Beachten Sie, der Controller wird ohne Speicherkarte ausgeliefert.
Für die Nutzung einer Speicherkarte müssen Sie diese separat dazu bestellen.
Der Controller kann auch ohne Speicherkartenerweiterung betrieben werden, die Verwendung einer Speicherkarte ist optional.

**Hinweis**

**Nur empfohlene Speicherkarte verwenden!**
Setzen Sie ausschließlich die von WAGO erhältliche und für den Controller vorgesehene Speicherkarte ein, da diese für industrielle Anwendungen unter erschwerten Umgebungsbedingungen und für den Einsatz in diesem Gerät spezifiziert ist.
Die Kompatibilität zu anderen im Handel erhältlichen Speichermedien kann nicht gewährleistet werden.

## 4.2 Schematisches Schaltbild

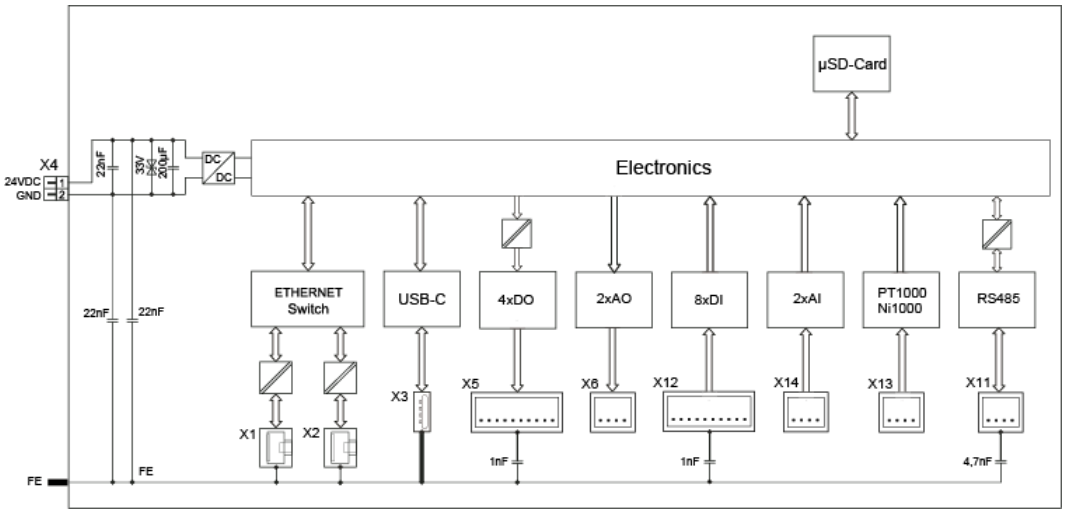



Abbildung 5: Schematisches Schaltbild

# 4.3 Technische Daten

## 4.3.1 Mechanische Daten

Tabelle 18: Technische Daten – Mechanische Daten

| | |
|---|---|
| Breite | 108 mm / 4.252 inch |
| Höhe | 90 mm / 3.543 inch |
| Tiefe ab Oberkante Tragschiene | 55 mm / 2.165 inch |
| Gewicht | 190 g |

## 4.3.2 Systemdaten

Tabelle 19: Technische Daten – Systemdaten

| | |
|---|---|
| CPU | Cortex A7, 650 MHz |
| Betriebssystem | Echtzeit-Linux® mit RT-Preemption-Patch |
| Speicherkartensteckplatz | Push/Push-Mechanismus, Abdeckungsklappe plombierbar |
| Speicherkartentyp | MicroSD bis 32 Gbyte<br>(Alle zugesicherten Eigenschaften sind nur in Verbindung mit den WAGO-Speicherkarten 758-879/000-3102 und 758-879/000-3108 gültig.) |

## 4.3.3 Versorgung

Tabelle 20: Technische Daten – Versorgung

| | |
|---|---|
| Eingangsspannung System $U_S$+ | DC 24 V (SELV, −15 … +20 %)<br>• Einspeisung über Verdrahtungsebene (*picoMAX*®-Anschluss) |
| Max. Stromaufnahme System $U_S$+ | 500 mA |
| Eingangsspannung Feld (Digitale Ausgänge) $U_{in}$+ | DC 24 V (−15 … +20 %)<br>• Einspeisung über Verdrahtungsebene (*picoMAX*®-Anschluss) |
| Max. Stromaufnahme Feld (Digitale Ausgänge) $U_{in}$+ | 2 A |
| Ausgangsspannung System $U_{out}$+ | DC 24 V (−15 … +20 %), nicht kurzschlussfest |
| Max. Stromabgabe System $U_{out}$+ | 200 mA |
| Potentialtrennung | 1250 V (DC 1 min.,<br>zwischen Systemebene und Feldebene (Digitale Ausgänge)) |
| Netzausfallzeit gemäß IEC 61131-2 | Abhängig von externer Pufferung |
| Verlustleistung bei 35 °C | |
| Normalbetrieb | 3,12 W |
| Volllast (gemäß technischen Daten) | 4,61 W |

**Hinweis**

**Für Systemversorgung externe Pufferung vornehmen!**
Zur Überbrückung von Netzausfallzeiten muss die Systemversorgung und bei Bedarf auch die Feldversorgung gepuffert werden.
Da der Strombedarf vom jeweiligen Knotenaufbau abhängt, ist die Pufferung nicht intern implementiert.
Um Netzausfallzeiten von 1 ms oder 10 ms gemäß IEC61131-2 zu erreichen, ermitteln Sie die für Ihren Knotenaufbau angemessene Pufferung und bauen Sie diese als externe Beschaltung auf.

### 4.3.4 Uhr

Tabelle 21: Technische Daten – Uhr

| | |
|---|---|
| Pufferzeit RTC (25 °C) | 6 Tage |

### 4.3.5 Programmierung

Tabelle 22: Technische Daten – Programmierung

| | |
|---|---|
| Programmierung | CODESYS V3 |
| IEC 61131-3 | KOP, FUP (CFC), ST, AS |
| Speicherkonfiguration | |
| Programmspeicher (Flash) | 32 MByte |
| Datenspeicher (RAM) | 128 MByte |
| Remanentspeicher (NVRAM, Retain + Merker) | 128 kByte |

### 4.3.6 ETHERNET

Tabelle 23: Technische Daten – ETHERNET

| | |
|---|---|
| ETHERNET | 2 x RJ-45 (switched oder separated Mode) |
| Übertragungsmedium | Twisted Pair S-UTP, 100 Ω, Cat 5, 100 m maximale Leitungslänge |
| Übertragungsrate | 10/100 Mbit/s; 10Base-T/100Base-TX |
| Protokolle | DHCP, DNS, SNTP, FTP, FTPS (nur explizite Verbindungen), SNMP, HTTP, HTTPS, SSH, Modbus (TCP), EtherCAT Master, EtherNet/IP-Adapter, EtherNet/IP-Scanner, OPC UA |

**Hinweis**

**Kein direkter Zugriff vom Feldbus auf das Prozessabbild der I/O-Module!**
Benötigte Daten aus dem OnBoard-I/O-Prozessabbild müssen explizit im Steuerungsprogramm auf die Daten im Feldbus-Prozessabbild gemappt werden und umgekehrt! Ein direkter Zugriff ist nicht möglich!

### 4.3.7 Kommunikationsschnittstelle

Tabelle 24: Technische Daten – Kommunikationsschnittstelle

| | |
|---|---|
| Schnittstelle | 1 x serielle Schnittstelle gemäß TIA/EIA 485, *picoMAX*® |
| Protokolle | abhängig vom IEC-Programm |
| Übertragungskanäle | 1 TxD / 1 RxD, halbduplex |
| Übertragungsrate | 115200 Baud |
| Potentialtrennung | ja |

### 4.3.8 Anschlusstechnik

Tabelle 25: Technische Daten – Verdrahtungsebene

| | |
|---|---|
| Anschlusstechnik | *picoMAX*® 3.5; Push-in CAGE CLAMP® |
| Betätigungsart | Drücker |
| Leiterquerschnitt eindrähtiger/feindrähtiger Leiter | 0,2 … 1,5 mm² / 24 … 14 AWG |
| Leiterquerschnitt feindrähtiger Leiter; mit Aderendhülse mit Kunststoffkragen | 0,25 … 0,75 mm² |
| Leiterquerschnitt feindrähtiger Leiter; mit Aderendhülse ohne Kunststoffkragen | 0,25 … 1,5 mm² |
| Abisolierlänge | 8 … 9 mm / 0.31 … 0.35 inch |
| Temperaturbeständigkeit der Leiter | min. 70 °C |

### 4.3.9 Digitale Eingänge

Tabelle 26: Technische Daten – Digitale Eingänge

| | |
|---|---|
| Anzahl digitale Eingänge | 8 |
| Eingangstyp | Typ 3 (IEC 61131-2), positivschaltend |
| Eingangssignal „0“ | DC –3 … +5 V |
| Eingangssignal „1“ | DC +11 …+30 V |
| Eingangsfilter | 5,0 µs |
| Typ. Eingangsstrom | 2,8 mA |

### 4.3.10 Digitale Ausgänge

Tabelle 27: Technische Daten – Digitale Ausgänge

| | |
|---|---|
| Anzahl digitale Ausgänge | 4 |
| Ausgangsspannung | DC 24 V |
| Lastarten | Gleichstromkreis, allgemeine Verwendung (gemäß UL 61010-2-201, Absatz 4.4.2.101) |
| Verpolungsschutz | ja |
| Max. Schaltfrequenz | 1 kHz |
| Max. Ausgangsstrom, 1 Ausgang | 0,5 A, kurzschlussfest |

### 4.3.11 Analoge Eingänge

Tabelle 28: Technische Daten – Analoge Eingänge

| | |
|---|---|
| Anzahl analoge Eingänge | 2 |
| Anschlussarten | single-ended |
| Eingangsspannung, Messbereich | 0 … 10 V |
| Max. Eingangsspannung | ±30 V |
| Typ. Eingangswiderstand | > 100 kΩ |
| Auflösung | 16 Bit |
| Temperaturkoeffizient | < ±0,01 %/K vom Skalenendwert |

### 4.3.12 Analoge Ausgänge

Tabelle 29: Technische Daten – Analoge Ausgänge

| | |
|---|---|
| Anzahl analoge Ausgänge | 2 |
| Ausgangsspannung, Messbereich | 0 … 10 V |
| Bürde | > 5 kΩ |
| Typ. Einschwingzeit | 100 ms |
| Auflösung | 12 Bit |
| Messfehler bei 25 °C | < ±0,2 % vom Skalenendwert |
| Temperaturkoeffizient | < ±0,005 %/K vom Skalenendwert |

### 4.3.13 Klimatische Umgebungsbedingungen

Tabelle 30: Technische Daten – Klimatische Umgebungsbedingungen

| | |
|---|---|
| Umgebungstemperaturbereich (Betrieb) | −25 … +60 °C |
| Umgebungstemperaturbereich (Lagerung) | −25 … +85 °C |
| Relative Feuchte (ohne Betauung) | 5 … 95 % |
| Betriebshöhe über NN | 2000 m |
| Verschmutzungsgrad | 2 |
| Überspannungskategorie | II |
| Schutzart | IP20 |
| Besondere Bedingungen | • Die Komponenten dürfen nicht ohne Zusatzmaßnahmen an Orten eingesetzt werden, an denen Staub, ätzende Dämpfe, Gase oder ionisierende Strahlung auftreten können.<br>• Der zulässige Temperaturbereich der Anschlussleitung muss abhängig von der Einbaulage und Stromstärke dimensioniert sein, da die Klemmstellentemperatur bis zu 25 K (bei 10 A) über der maximal zu erwartenden Umgebungs-temperatur liegen kann. |

Die zulässigen Umgebungstemperaturen in Abhängigkeit zu den Einbaulagen finden Sie im Kapitel „Montieren“ > „Einbaulage“.

### 4.3.14 Analoge Temperatursensoren

Tabelle 31: Technische Daten – Analoge Temperatursensoren

| | |
|---|---|
| Anzahl der Eingänge | 2 |
| Sensorarten | Umschaltbar: Pt1000, Ni1000 oder Rohwert (450 … 4400 Ohm) |
| Temperaturbereich | |
| Pt | –60 … +350 °C |
| Ni | –60 … +350 °C |
| Typ. Messstrom | 0,5 mA |
| Anschlussarten | 2-Leiter-Anschluss |
| Auflösung über gesamten Bereich | 16 Bit |
| Messgenauigkeit Pt1000 bei 25 °C | < ±0,5 % hardwaretechnisch |
| Messgenauigkeit Ni1000 bei 25 °C | < ±0,5 % hardwaretechnisch |
| Temperaturkoeffizient | < ±0,02 % / K vom Skalenendwert |

### 4.3.15 Feldbus

Tabelle 32: Technische Daten – Feldbus

| | |
|---|---|
| Unterstützte Protokolle (lizenzfrei) | Modbus TCP (Client/Server) gemäß CODESYS, Modbus RTU (Master/Slave) gemäß CODESYS, Cloud Connectivity (1. Verbindung), EtherCAT Master, EtherNet/IP-Adapter, EtherNet/IP-Scanner, OPC UA |
| Unterstützte Protokolle (lizenzpflichtig) | Cloud Connectivity (2. Verbindung per DRM), MQTT Sparkplug (per DRM), BACnet/IP (per DRM), Telecontrol (IEC 60870, IEC 61850, DNP3) (per DRM) |
| Unterstützte Gateways (lizenzfrei) | Gateway Modbus TCP zu Modbus RTU gemäß CODESYS |

### 4.3.16 Sonstiges

Tabelle 33: Technische Daten – Sonstiges

| | |
|---|---|
| Brandlast | 5,890 MJ |

## 4.4 Zulassungen

Folgende Zulassungen wurden für den Controller „Compact Controller 100“ (751-9301) erteilt:

| | | |
|---|---|---|
|  | Konformitätskennzeichnung | |
|  | UK Conformity Assessed | |
|  | Ordinary Locations | UL61010-2-201 |
|  | Korea Certification: R-R-W43-CC751 | |

## 4.5 Normen und Richtlinien

Der Controller „Compact Controller 100“ (751-9301) erfüllt folgende EMV-Normen:

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

# 5 Funktionsbeschreibung

## 5.1 Netzwerk

### 5.1.1 Schnittstellenkonfiguration

Die Netzwerkschnittstellen X1 und X2 des Controllers sind mit einem integrierten, konfigurierbaren 3-Port-Switch verbunden, dessen dritter Port mit der CPU verbunden ist.

Die zwei Schnittstellen und der konfigurierbare Switch ermöglichen die Verdrahtung:

- in einem gemeinsamen Netzwerk mit einer gemeinsamen IP-Adresse für beide Schnittstellen oder
- in zwei getrennten Netzwerken mit einer eigenen IP-Adresse für jede Schnittstelle.

Die Zuordnung der physikalischen Schnittstellen (Ports) erfolgt dabei über logische Bridges und kann z. B. über das WBM konfiguriert werden.


Abbildung 6: Beispiel für Schnittstellenzuordnung über WBM

Für das Interface X1 kann temporär eine feste IP-Adresse („Fix IP Address“-Modus) eingestellt werden. Die Einstellung erfolgt mit dem Reset-Taster (siehe Kapitel „In Betrieb nehmen“ > …> „Temporär eine feste IP-Adresse einstellen“).

Die Einstellung einer temporären festen IP-Adresse hat keine Auswirkung auf den zuvor eingestellten Modus.

#### 5.1.1.1 Betrieb im Switch-Modus

Für den Betrieb im Switch-Modus gelten die TCP/IP-Einstellungen wie die IP-Adresse oder die Subnetzmaske sowohl für X1 als auch für X2.

Beim Umschalten in den Switch-Modus werden die Einstellungen von X1 als neue gemeinsame Konfiguration für X1 und X2 übernommen.
Das Gerät ist dann über die vormals für X2 eingestellte IP-Adresse nicht mehr erreichbar. Für Applikationen, die X2 zur Kommunikation nutzen, muss dies berücksichtigt werden.

#### 5.1.1.2 Betrieb mit getrennten Netzwerk-Schnittstellen

Im Betrieb mit getrennten Netzwerk-Schnittstellen können die beiden ETHERNET-Schnittstellen separat konfiguriert und eingesetzt 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.

### 5.1.1.3 Beispiele für die Zuordnung der MAC-IDs und IP-Adressen

#### Ein gemeinsames Netzwerk mit einer gemeinsamen IP-Adresse für alle 2 Schnittstellen


Abbildung 7: 1 Bridge mit 2 Ports

Tabelle 34: Zuordnung der MAC-IDs und IP-Adressen für 1 Bridge mit 2 Ports

| Bridge | MAC-ID | IP-Adr. | Port | MAC-ID | Port | MAC-ID |
|---|---|---|---|---|---|---|
| 1 | 01 | 1 | X1 | 02 | X2 | 03 |

#### Zwei getrennte Netzwerke mit einer eigenen IP-Adresse für jede Schnittstelle

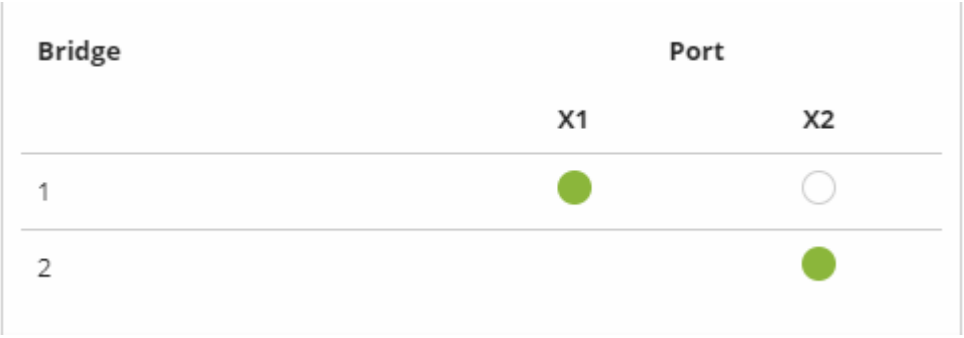



Abbildung 8: 2 Bridges mit 1/1 Ports

Tabelle 35: Zuordnung der MAC-IDs und IP-Adressen für 2 Bridges mit 1/1 Ports

| Bridge | MAC-ID | IP-Adr. | Port | MAC-ID | Port | MAC-ID |
|---|---|---|---|---|---|---|
| 1 | 01 | 1 | X1 | 01 | | |
| 2 | 02 | 2 | | | X2 | 02 |

## 5.1.2 Netzwerksicherheit

### 5.1.2.1 Benutzer und Passwörter

Im Controller gibt es 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!

#### 5.1.2.1.1 Dienste und Benutzer

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

Tabelle 36: Dienste und Benutzer

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

#### 5.1.2.1.2 WBM-Benutzergruppe

Das WBM hat eine eigene Benutzerverwaltung. Die hier verwendeten Benutzer sind aus Sicherheitsgründen von den übrigen Benutzergruppen im System isoliert.

Tabelle 37: WBM-Benutzer

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

**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.

**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!

Weitere Informationen finden Sie im Kapitel „Benutzerverwaltung des WBM“.

#### 5.1.2.1.3 Linux®-Benutzergruppe

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

Tabelle 38: Linux®-Benutzer

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

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

**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!

#### 5.1.2.1.4 SNMP-Benutzergruppe

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

#### 5.1.2.2 Webserverauthentifizierung

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

Die Standardeinstellung des Controllers ermöglicht starke Verschlüsselung, nutzt aber nur einfache Authentifizierungsverfahren. Da eine Authentifizierung für alle sicheren Kommunikationskanäle eine zentrale Rolle spielt, ist dringend angeraten, eine sicherere Authentifizierung durchzuführen. Basis der Authentifizierung bildet das auf dem Controller gespeicherte Sicherheitszertifikat. Der Standardablageort des Sicherheitszertifikats ist: /etc/lighttpd/https-cert.pem.

Im Auslieferzustand verwendet der Controller ein generisches Sicherheitszertifikat im x509-Format. Um eine sicherere Authentifizierung zu ermöglichen, müssen Sie dieses generische Sicherheitszertifikat durch ein spezifisches für das individuelle Gerät ersetzen.

##### 5.1.2.2.1 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 und starke Algorithmen. Ältere Software und ältere Betriebssysteme unterstützen eventuell TLS 1.2 und die Verschlüsselungsalgorithmen nicht.
Mit der Einstellung „Standard“ sind TLS 1.0, TLS 1.1, TLS 1.2 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**

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

#### 5.1.2.3 Root-Zertifikate

Bei mittels TLS verschlüsselter Kommunikation werden zur Überprüfung der Authentizität des Kommunikationspartners Root-Zertifikate verwendet.
Ein Root-Zertifikat, welches von einer Zertifizierungsstelle signiert wurde, dient dazu, die Gültigkeit aller Zertifikate zu verifizieren, die von dieser Zertifizierungsstelle ausgestellt wurden.

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

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

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

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

Die Root-Zertifikate können durch Aktualisierung der Datei /etc/ssl/certs/ca-certificates.crt auf dem Controller aktualisiert werden (siehe Kapitel „Service“ > „Root-Zertifikate aktualisieren“).

## 5.1.3 Netzwerkkonfiguration

### 5.1.3.1 Hostname/Domainname

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

### 5.1.3.2 Routing

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

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

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

Anhand des eingestellten Zielsystems, bestehend aus Destination-Address und Destination-Mask, wird entschieden, an welches Gateway ein Netzwerk-

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

**Default-Gateway:**
Wird im Feld „Destination-Address“ der Wert „default“ eingetragen, so wird ein Default-Gateway, auch Default-Route genannt, definiert. Im Feld Destination-Mask muss dann der Wert „0.0.0.0“ gesetzt werden.

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

Liegt die IP-Adresse des Gateways außerhalb des vom Controller erreichbaren IP-Adressraums, wird die zugehörige Route nicht aktiviert.

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

Die Metrik der konfigurierten Routing-Einträge kann für den Controller vorgegeben werden. Der Standardwert für die Metrik ist 20. Neben den manuell konfigurierbaren Routen können Default-Gateways durch DHCP-Antworten eingestellt werden. Alle per DHCP übergebenen Default-Gateways bekommen unveränderbar eine Metrik von 10 zugeordnet.

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

Über die Routing-Einträge wird konfiguriert, an welche Gateways die Netzwerk-Datenpakete gesendet werden. Wird der Controller im Switched-Mode betrieben und besitzt nur ein Netzwerk-Interface, verläuft sämtlicher Netzwerkverkehr über dieses Netzwerk-Interface. Wird der Controller im Separated-Mode betrieben

oder enthält der Controller ein Modem, besitzt er mehr als ein Netzwerk-Interface. Damit ist es möglich, dass ein Netzwerk-Datenpaket den Controller auf einem Netzwerk-Interface erreicht und auf einem anderen Netzwerk-Interface wieder verlässt. Diese Weiterleitung zwischen verschiedenen Netzwerk-Interfaces muss explizit freigeschaltet werden und ist im Auslieferungszustand deaktiviert. Um die Weiterleitung zu aktivieren, muss „Routing enabled entirely“ in der Gruppe „General Routing Configuration“ aktiviert werden. In diesem Fall kann der Controller als Router fungieren.

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

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

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

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

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

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

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

## 5.1.4 Netzwerkdienste

### 5.1.4.1 DHCP-Client

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

Folgende Parameter können bezogen werden:

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

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

Die Parameter Hostname und Domain werden jeweils nach dem LIFO-Prinzip (Last In First Out) gespeichert. Es werden immer die Einstellungen des zuletzt empfangenen DHCP-Offers verwendet.

Die Parameter DNS- und NTP-Server werden zur globalen Verwendung zentral gespeichert. Es werden alle übertragenen Parameter gespeichert.

## 5.1.5 Cloud-Connectivity-Funktionalität

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

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

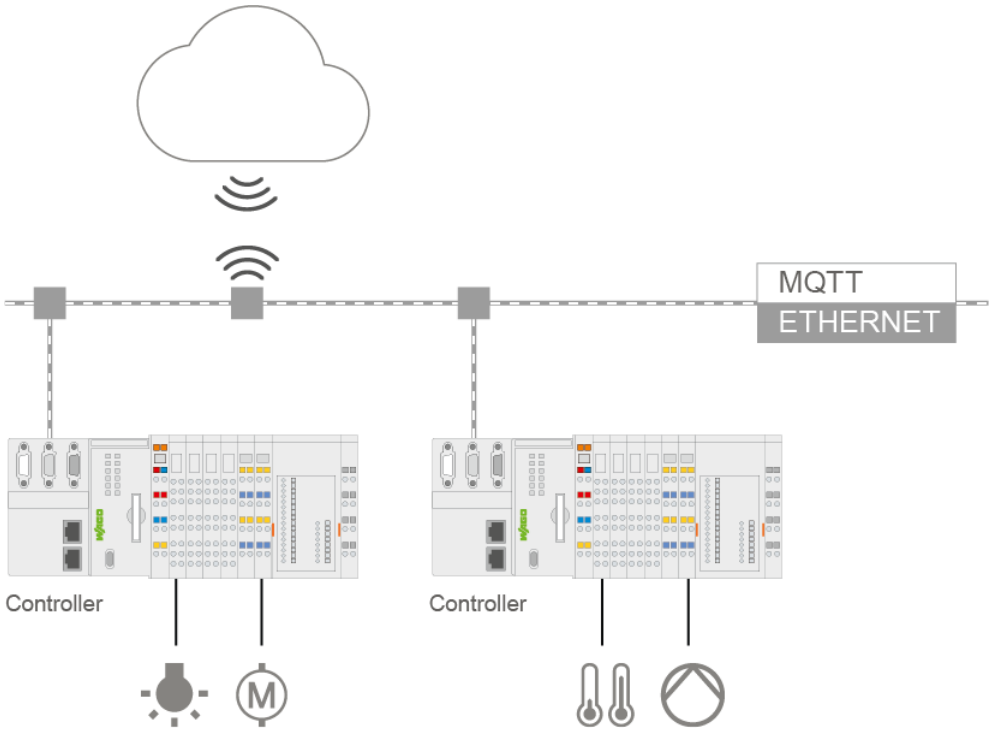



Abbildung 9: Anbindung der Controller an einen Cloud-Dienst (Beispiel)

Die Daten werden vom Controller zum Cloud-Dienst im JSON-Format übertragen. Die Verbindung kann per TLS verschlüsselt werden, siehe hierzu Kapitel „Funktionsbeschreibung“ > … > „TLS-Verschlüsselung“.

Einstellungen, die im Controller für die Nutzung der Cloud-Connectivity-Funktionalität vorgenommen werden müssen, finden Sie im Kapitel „In Betrieb nehmen“ > … > „Konfiguration mittels Web-Based-Management“.

Die Konfiguration der Kommunikationsparameter erfolgt im WBM, die Konfiguration der zwischen Cloud und Controller auszutauschenden Daten erfolgt mit der CODESYS V3-Bibliothek „WagoAppCloud“.

**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.

**Information**

**Beachten Sie die zusätzlichen Dokumentationen!**
Eine detaillierte Beschreibung des Softwarepaketes Cloud-Connectivity mit einem Controller und Informationen zur SPS-Programmierung finden Sie im Anwendungshinweis A500920 im Downloadbereich unter www.wago.com.

**Information**

**Beachten Sie die erforderlichen Einstellungen zu Datenschutz und Sicherheit!**
Bevor Sie die Cloud-Connectivity-Funktionalität nutzen, informieren Sie sich zum Thema Datenschutz und Sicherheit in dem entsprechenden Handbuch. Dieses finden Sie im Downloadbereich unter www.wago.com.

#### 5.1.5.1 Komponenten des Softwarepaketes Cloud-Connectivity

Tabelle 39: Komponenten des Softwarepaketes Cloud-Connectivity

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

## 5.2 Speicherkartenfunktion

**Hinweis**

**Nur empfohlene Speicherkarte verwenden!**
Setzen Sie ausschließlich die von WAGO erhältliche und für den Controller vorgesehene Speicherkarte ein, da diese für industrielle Anwendungen unter erschwerten Umgebungsbedingungen und für den Einsatz in diesem Gerät spezifiziert ist.
Die Kompatibilität zu anderen im Handel erhältlichen Speichermedien kann nicht gewährleistet werden.

Die Speicherkarte ist optional und dient als zusätzlicher Speicherbereich zu dem internen Speicher bzw. Laufwerk in dem Controller. Auf die Speicherkarte können das Anwenderprogramm, Anwenderdaten, der Quellcode des Projektes oder Geräteeinstellungen gespeichert werden und damit auch bereits bestehende Projektdaten und Programme auf einen oder mehrere Controller kopiert werden.

Ist die Speicherkarte eingefügt, wird diese unter /media/sd in die Verzeichnisstruktur des controllerinternen Dateisystems eingebunden. Somit kann die Speicherkarte wie ein Wechselmedium an einem PC angesprochen werden.

Die Funktion der Speicherkarte im Normalbetrieb und mögliche Störungen, die beim Einsatz der Speicherkarte auftreten können, werden in den jeweiligen nachfolgenden Kapiteln für verschiedene Abschnitte des Betriebes beschrieben.

### 5.2.1 Formatierung

**Hinweis**

**Vorformatierung der Speicherkarte 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“ oder „NTFS“.

## 5.2.2 Datensicherung

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

Über die WBM-Seiten „Backup“ und „Restore“ können die notwendigen Einstellungen vorgenommen und die Funktionen ausgeführt werden.

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

Weiterhin können die zu sichernden und wiederherzustellenden Daten ausgewählt werden:

- das CODESYS Projekt („PLC-Runtime-Projekt“, Boot-Projekt)
- die Geräteeinstellungen („Settings“)
- das Controllerbetriebssystem („System“)
- alle vorherigen, („All“, nur sichtbar, wenn nicht im Netzwerk gespeichert wird)

**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.

### 5.2.2.1 Backup-Funktion

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

Die Backup-Funktion kann über die WBM-Seite „Firmware Backup“ aufgerufen werden.

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

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

Wenn die Speicherkarte als Zielmedium ausgewählt ist, blinkt die LED über dem Speicherkartensteckplatz während des Speichervorgangs gelb.

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

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

**Hinweis**

**Nur ein Package zum Netzwerk kopierbar!**
Wenn Sie „Network“ als Speicherziel eingestellt haben, ist je Speichervorgang nur ein Package auswählbar.

**Hinweis**

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

**Hinweis**

**Backup-Zeit berücksichtigen**
Das Erzeugen der Backup-Dateien kann einige Minuten dauern. Stoppen sie vor dem Backup-Vorgang das CODESYS Programm, um diese Zeit weiter zu verkürzen.

#### 5.2.2.2 Restore-Funktion

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

Die Restore-Funktion kann über die WBM-Seite „Firmware Restore“ aufgerufen werden.

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

Wenn die Speicherkarte als Quellmedium ausgewählt ist, blinkt die LED über dem Speicherkartensteckplatz während des Ladevorgangs gelb.

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

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

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

WBM-Seite „PLC Runtime Configuration“ im Register „Configuration“, Auswahl „PLC Runtime“ aufgerufen werden.

**Hinweis**

**Datengröße darf nicht größer als die interne Laufwerksgröße sein!**
Beachten Sie, dass die Größe der Daten in dem Verzeichnis media/sd/copy die Gesamtgröße des internen Laufwerks nicht überschreiten darf.

**Hinweis**

**Wiederherstellung nur vom internen Speicher möglich!**
Wenn das 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.

### 5.2.3 Einfügen einer Speicherkarte im Betrieb

Der Feldbusknoten und das SPS-Programm sind in Betrieb.

Sie legen eine Speicherkarte im laufenden Betrieb ein.

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

Die LED über der Speicherkarte blinkt während des Zugriffs gelb.

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

### 5.2.4 Entfernen der Speicherkarte im Betrieb

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

Sie ziehen die Speicherkarte im laufenden Betrieb heraus.

**Hinweis**

**Daten können beim Schreiben verloren gehen!**
Beachten Sie, dass bei dem Herausziehen der Speicherkarte während eines Schreibzugriffes Daten verloren gehen.

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

Der Controller arbeitet anschließend ohne Speicherkarte.

### 5.2.5 Einstellung des Home-Verzeichnisses für das Laufzeitsystem

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

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

Die Einstellung kann über das Kontrollfeld „Home directory on memory card enabled“ auf der WBM-Seite „PLC Runtime“ erfolgen. Sie wird durch Klicken der Schaltfläche **[Submit]** übernommen und nach dem nächsten Neustart wirksam. Es werden keine Dateien vom alten in das neue Home-Verzeichnis übernommen.

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

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

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

### 5.2.6 Boot-Projekt laden

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

Tabelle 40: Laden eines Boot-Projekts

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

# 6 Montieren

## 6.1 Einbaulage

Je nach Einbaulage und Abstand (D) des Produktes zur Spannungsversorgung (siehe Kapitel „Montieren“ > „Abstände“) ergeben sich unterschiedliche zulässige Umgebungstemperaturen.
Folgende Einbaulagen sind erlaubt:

Tabelle 41: Einbaulagen und zulässige Umgebungstemperaturen

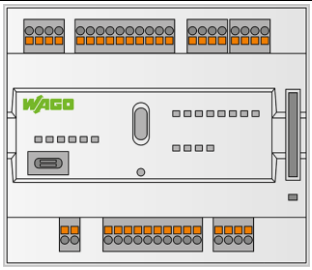
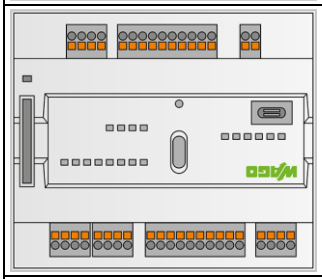
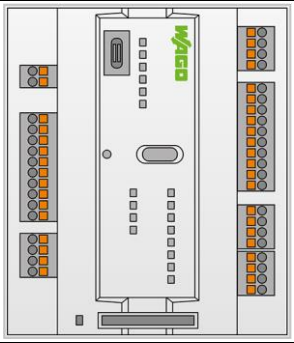
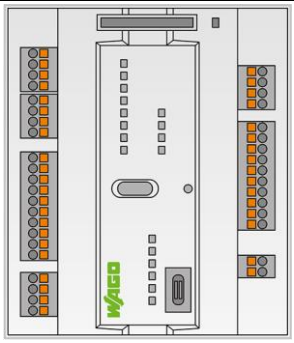
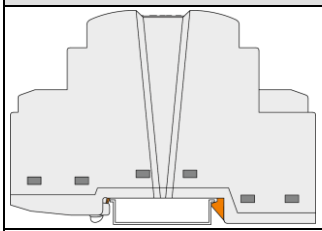
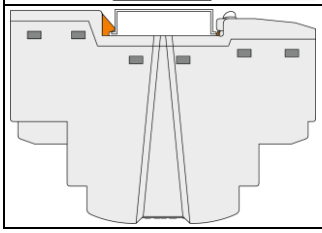
| Abbildung | Einbaulage | Zulässige Umgebungstemperatur |
|---|---|---|
|  | Horizontal (Standard) | D = 10 mm: –25 … +60 °C<br>D = 0 mm: –25 … +55 °C |
|  | Horizontal 180 ° | D = 0 mm: –25 … +55 °C |
|  | Vertikal | D = 0 mm: –25 … +55 °C |
|  | Vertikal 180 ° | D = 0 mm: –25 … +50 °C |

Tabelle 41: Einbaulagen und zulässige Umgebungstemperaturen

| Abbildung | Einbaulage | Zulässige Umgebungstemperatur |
|---|---|---|
|  | Bodenmontage | D = 0 mm: –25 … +50 °C |
|  | Überkopfmontage | D = 0 mm: –25 … +50 °C |

**Hinweis**

**Bei vertikalem Einbau Endklammer verwenden!**

Montieren Sie beim vertikalen Einbau zusätzlich unterhalb des Feldbusknotens eine Endklammer, um den Feldbusknoten gegen Abrutschen zu sichern.

WAGO-Bestellnummer 249-116 Endklammer für TS 35, 6 mm breit

WAGO-Bestellnummer 249-117 Endklammer für TS 35, 10 mm breit

# 6.2 Montage auf Tragschiene

## 6.2.1 Tragschieneneigenschaften

Alle Komponenten des Systems können direkt auf eine Tragschiene gemäß EN 60175 (TS 35, DIN Rail 35) aufgerastet werden.

**ACHTUNG**

**Ohne Freigabe keine WAGO fremden Tragschienen verwenden!**
WAGO GmbH & Co. KG liefert normkonforme Tragschienen, die optimal für den Einsatz mit dem WAGO I/O SYSTEM geeignet sind. Sollten Sie andere Tragschienen einsetzen, muss eine technische Untersuchung und eine Freigabe durch WAGO GmbH & Co. KG vorgenommen werden.

Tragschienen weisen unterschiedliche mechanische und elektrische Merkmale auf. Für den optimalen Aufbau des Systems auf einer Tragschiene sind Randbedingungen zu beachten:

- Das Material muss korrosionsbeständig sein.
- Die meisten Komponenten besitzen zur Ableitung von elektromagnetischen Einflüssen einen Ableitkontakt zur Tragschiene. Um Korrosionseinflüssen vorzubeugen, darf dieser verzinnte Tragschienenkontakt mit dem Material der Tragschiene kein galvanisches Element bilden, das eine Differenzspannung über 0,5 V (Kochsalzlösung von 0,3 % bei 20 °C) erzeugt.
- Die Tragschiene muss die im System integrierten EMV-Maßnahmen und die Schirmung optimal unterstützen.
- Eine ausreichend stabile Tragschiene ist auszuwählen und ggf. mehrere Montagepunkte (alle 20 cm) für die Tragschiene zu nutzen, um Durchbiegen und Verdrehung (Torsion) zu verhindern.
- Die Geometrie der Tragschiene darf nicht verändert werden, um den sicheren Halt der Komponenten sicherzustellen. Insbesondere beim Kürzen und Montieren darf die Tragschiene nicht gequetscht oder gebogen werden.
- Der Rastfuß der Komponenten reicht in das Profil der Tragschiene hinein. Bei Tragschienen mit einer Höhe von 7,5 mm sind Montagepunkte (Verschraubungen) unter dem Knoten in der Tragschiene zu versenken (Senkkopfschrauben oder Blindnieten).
- Die Metallfedern auf der Gehäuseunterseite müssen einen niederimpedanten Kontakt zur Tragschiene haben (möglichst breitflächige Auflage).

### 6.2.2 WAGO Tragschienen

Die WAGO Tragschienen erfüllen die elektrischen und mechanischen Anforderungen.

Tabelle 42: WAGO Tragschienen

| Bestellnr. | Beschreibung |
|---|---|
| 210-112 | 35 × 7,5; 1 mm; Stahl; bläulich, verzinkt, chromatiert; gelocht |
| 210-113 | 35 × 7,5; 1 mm; Stahl; bläulich, verzinkt, chromatiert; ungelocht |
| 210-197 | 35 × 15; 1,5 mm; Stahl; bläulich, verzinkt, chromatiert; gelocht |
| 210-114 | 35 × 15; 1,5 mm; Stahl; bläulich, verzinkt, chromatiert; ungelocht |
| 210-118 | 35 × 15; 2,3 mm; Stahl; bläulich, verzinkt, chromatiert; ungelocht |
| 210-198 | 35 × 15; 2,3 mm; Kupfer; ungelocht |
| 210-196 | 35 × 8,2; 1,6 mm; Aluminium; ungelocht |

**ACHTUNG**

**Bei erhöhter Beanspruchung Befestigungsabstand der Tragschiene beachten!**
Montieren Sie die Tragschiene bei erhöhter Vibrations- und Schockbeanspruchung mit einem Befestigungsabstand von maximal 60 mm.

## 6.3 Abstände

Für den gesamten Feldbusknoten muss grundsätzlich ein Mindestabstand von min. 35 mm zu Kabelkanälen und Gehäuse-/Rahmenwänden eingehalten werden. Der Abstand (D) zur Spannungsversorgung beträgt, je nach Einbaulage, 0 … 10 mm (siehe Kapitel „Montieren“ > „Einbaulage“).
Für auf der Tragschiene benachbarte Komponenten kann ggf. dieser Mindestabstand unterschritten werden.

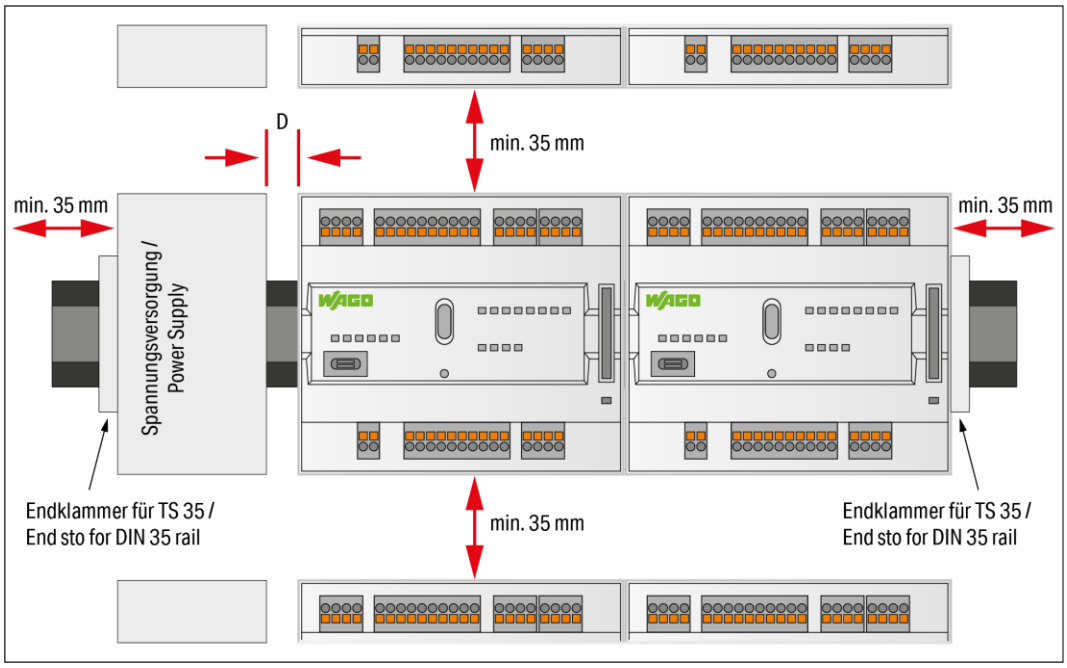



Abbildung 10: Abstände

Die Abstände schaffen Raum zur Wärmeableitung und Montage bzw. Verdrahtung. Ebenso verhindern die Abstände zu Kabelkanälen, dass leitungsgebundene elektromagnetische Störungen den Betrieb beeinflussen.

Bei eingeschränktem Bauraum im Schaltschrank oder Installationskleinverteiler, verwenden Sie für die Netzwerkanschlüsse X1 und X2, bei Bedarf, abgewinkelte Netzwerkkabel oder Patchkabel.

# 6.4 Geräte einfügen

**GEFAHR**

**Nicht an Geräten unter Spannung arbeiten!**
Gefährliche elektrische Spannung kann zu elektrischem Schlag und Verbrennungen führen.
Schalten Sie immer alle verwendeten Spannungsversorgungen für das Gerät ab, bevor Sie das Gerät montieren, installieren, Störungen beheben oder Wartungsarbeiten vornehmen.

## 6.4.1 Controller einfügen

Rasten Sie den Controller auf die Tragschiene auf.

Die Rastfußentriegelung springt automatisch zurück in das Gehäuse, sobald der Controller auf der Tragschiene eingerastet ist.

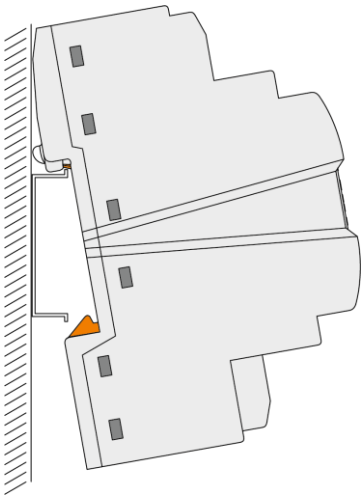


Abbildung 11: Controller einfügen

## 6.4.2 WAGO Steckverbinder *picoMAX*®

Mit Hilfe der steckbaren WAGO Steckverbinder *picoMAX*® können Sie die Geräte vorverdrahten und damit die Installationszeiten der Geräte verkürzen sowie ein Umverdrahten beim Austausch des Gerätes vermeiden.

Die WAGO Steckverbinder *picoMAX*® bestehen jeweils aus einer Stiftleiste (fest im Gerät verankert) und einer Federleiste (steckbar).

Weitere Informationen zu *picoMAX*® finden Sie im Katalog „*picoMAX*® – Das Steckverbindersystem“ oder im Internet unter www.wago.com.

### 6.4.2.1 Lieferzustand

Im Lieferzustand sind die Federleisten nicht im Gerät gesteckt, werden aber mitgeliefert.

### 6.4.2.2 Ziehen der Federleiste

WAGO empfiehlt die Benutzung des Entriegelungswerkzeuges *picoMAX*® (im Weiteren als „Entriegelungswerkzeug“ bezeichnet). Weitere Informationen zum Entriegelungswerkzeug finden Sie im Kapitel „Zubehör“ > „Werkzeuge“.

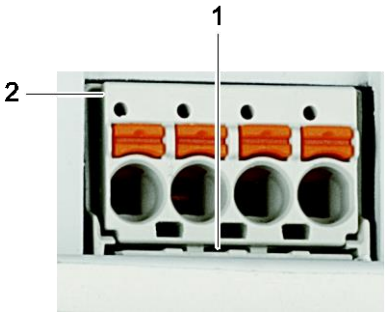



Abbildung 12: Ziehen der Federleiste ohne Verdrahtung (Anwendungsbeispiel)

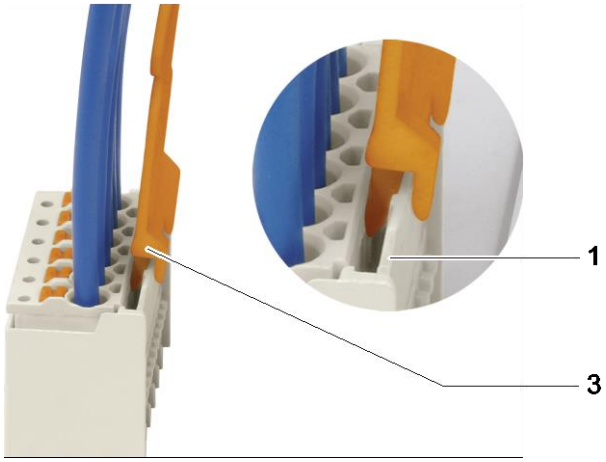



Abbildung 13: Ziehen der Federleiste mit Verdrahtung (Anwendungsbeispiel)

Tabelle 43: Legende zu den Abbildungen „Ziehen der Federleiste …“

| Position | Beschreibung |
|---|---|
| 1 | Rastlasche |
| 2 | Vorspringender Kragen der Federleiste |
| 3 | Entriegelungswerkzeug |

#### 6.4.2.2.1 Ziehen der Federleiste ohne Verdrahtung

Gehen Sie zum Ziehen der Federleiste mit dem Entriegelungswerkzeug wie folgt vor:

1. Stecken Sie das Entriegelungswerkzeug (3) auf die Rastlasche (1) auf.

2. Führen Sie das Entriegelungswerkzeug bis zum Anschlag ein.
   Der Keil am Entriegelungswerkzeug öffnet die Rastlasche, und die Verriegelung wird freigegeben (siehe auch Abbildung „Ziehen der Federleiste mit Verdrahtung“).

3. Fassen Sie unter den vorspringenden Kragen der Federleiste (2).

4. Ziehen Sie die Federleiste heraus.

Falls Sie kein Entriegelungswerkzeug zur Hand haben, können Sie die Federleiste auch mit Hilfe eines WAGO Betätigungswerkzeuges oder eines Schraubendrehers ziehen.

**WARNUNG**

**Werkzeug nicht in die Belüftungsschlitze stecken!**
Gelangt die Klinge des benutzten Werkzeuges durch die Belüftungsschlitze, können Komponenten im Inneren des Gerätes beschädigt werden. Dadurch kann es zu schwerwiegenden Folgeschäden mit Verletzungsgefahr durch Fehlfunktionen, zu hohe Wärmeentwicklung oder elektrischen Strom führen!

Beachten Sie beim Einsatz eines Schraubendrehers oder eines Betätigungswerkzeuges die korrekte Positionierung zwischen Rastlasche und Federleiste!

Gehen Sie wie folgt vor:

1. Drücken Sie mit dem Schraubendreher oder Betätigungswerkzeug die Rastlasche (1) weg von der Federleiste.

2. Fassen Sie unter den vorspringenden Kragen der Federleiste (2).

3. Ziehen Sie die Federleiste heraus.

#### 6.4.2.2.2 Ziehen der Federleiste mit Verdrahtung

Gehen Sie zum Ziehen der Federleiste mit dem Entriegelungswerkzeug wie folgt vor:

1. Stecken Sie das Entriegelungswerkzeug (3) auf die Rastlasche (1) auf.

2. Führen Sie das Entriegelungswerkzeug bis zum Anschlag ein.
Der Keil am Entriegelungswerkzeug öffnet die Rastlasche, und die Verriegelung wird freigegeben.

3. Ziehen Sie das Entriegelungswerkzeug gemeinsam mit den Leitern und der Federleiste heraus.

Falls Sie kein Entriegelungswerkzeug zur Hand haben, können Sie die Federleiste auch mit Hilfe eines WAGO Betätigungswerkzeuges oder eines Schraubendrehers ziehen.

**WARNUNG**

**Werkzeug nicht in die Belüftungsschlitze stecken!**
Gelangt die Klinge des benutzten Werkzeuges durch die Belüftungsschlitze, können Komponenten im Inneren des Gerätes beschädigt werden. Dadurch kann es zu schwerwiegenden Folgeschäden mit Verletzungsgefahr durch Fehlfunktionen, zu hohe Wärmeentwicklung oder elektrischen Strom führen!

Beachten Sie beim Einsatz eines Schraubendrehers oder eines Betätigungswerkzeuges die korrekte Positionierung zwischen Rastlasche und Federleiste!

**ACHTUNG**

**Bei Verwendung von Schraubendreher oder Betätigungswerkzeug nicht an den Leitern ziehen!**
Falls Sie zum Ziehen einen Schraubendreher bzw. ein Betätigungswerkzeug verwenden, dürfen Sie **nicht** an den Leitern ziehen!

Fassen Sie zum Herausziehen der Federleiste unter den vorspringenden Kragen der Federleiste!

### 6.4.2.3 Stecken der Federleiste

**Hinweis**

**Korrekten Steckplatz der *picoMAX*®-Federleisten beachten!**
Achten Sie beim Stecken auf den korrekten Steckplatz der jeweiligen Federleiste!

Zum Stecken der Federleiste in die zugehörige Stiftleiste gehen Sie wie folgt vor:

1. Stecken Sie die Federleiste in die entsprechende Stiftleiste.

**Hinweis**

**Ausrichtung beachten!**
Beachten Sie beim Stecken die richtige Ausrichtung der Federleiste:
Die orangefarbenen Drücker müssen zur Innenseite des Gehäuses zeigen.

2. Drücken Sie die Federleiste so weit in die Stiftleiste, bis die Federleiste hörbar einrastet.

3. Beim Stecken mit Verdrahtung: Prüfen Sie den festen Sitz der Federklemme durch kurzes, leichtes Ziehen an den Leitern.

# 7 Anschließen

## 7.1 Erden

Die Erdung erfolgt über die Federkontakte auf der Unterseite des Produktes durch Aufrasten auf die geerdete Tragschiene, siehe Abbildung in „Montieren“ > „Controller einfügen“.

## 7.2 Geräte anschließen

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.

**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.

**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.

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.

Der Controller nutzt die feste IP-Adresse 192.168.42.42, um mit einem PC zu kommunizieren.

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 X4, Pin 1 ($U_S$+) und 2 (GND) an. Verwenden Sie dazu ebenfalls den mitgelieferten Stecker (Federleiste 2091-1122).

# 8 In Betrieb nehmen

## 8.1 Einschalten des Controllers

Überprüfen Sie vor Einschalten des Controllers, dass Sie

- den Controller ordnungsgemäß montiert haben (siehe Kapitel „Montieren“),
- alle benötigten Datenleitungen (siehe Kapitel „Anschlüsse“) an die entsprechenden Schnittstellen angeschlossen haben,
- die Elektronik- und Feldversorgung angeschlossen haben (siehe Kapitel „Anschlüsse“),
- einen angemessenen Potentialausgleich an Ihrer Maschine/Anlage durchgeführt haben und
- die Schirmung ordnungsgemäß durchgeführt haben.

Zum Einschalten des Controllers schalten Sie an Ihrem Netzteil die Versorgungsspannung ein.

Das Starten des Controllers wird durch ein kurzes Aufleuchten der LEDs signalisiert. Nach einigen weiteren Sekunden signalisiert die SYS-LED den erfolgreichen Bootvorgang des Controllers.
Gleichzeitig wird das Laufzeitsystem CODESYS V3 gestartet.

Wurde das gesamte System erfolgreich gestartet, leuchtet die SYS-LED grün.

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

Ist kein ausführbares Programm im Controller gespeichert oder steht der Betriebsartenschalter auf STOP, wird dies ebenfalls durch RUN-LED angezeigt (siehe Kapitel „Diagnose“).

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

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

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

1. Öffnen Sie die Eingabeaufforderung.
   Geben Sie dazu im Eingabefeld unter **Start** > **Windows-System** > **Ausführen** (Windows® 10) oder **Start** > **Programme/Dateien durchsuchen** (Windows® 7) den Befehl „cmd“ ein.

2. Bestätigen Sie die Eingabe mit der Schaltfläche **[OK]** oder der **[Enter]**-Taste.

3. Geben Sie in der Eingabeaufforderung den Befehl „ipconfig“ ein.

4. Bestätigen Sie die Eingabe mit der **[Enter]**-Taste. Es erscheinen die IP-Adresse, Subnetzmaske und das Standard-Gateway mit den dazugehörigen Parametern.

# 8.3 Einstellen einer IP-Adresse

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

Tabelle 44: Voreingestellte IP-Adressierungen der Ethernet-Schnittstellen

| Ethernet-Schnittstelle | Voreinstellung |
|---|---|
| X1/X2<br>(Switched Mode) | Dynamische Vergabe der IP-Adresse mittels DHCP<br>(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 45: 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 |

### 8.3.1 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.

## 8.3.2 Ändern einer IP-Adresse mit „WAGO Ethernet Settings“

**Hinweis**

**WAGO Ethernet Settings-Version beachten!**
Das Produkt ist kompatibel ab der WAGO Ethernet Settings-Version 06.15.03.02.

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“.

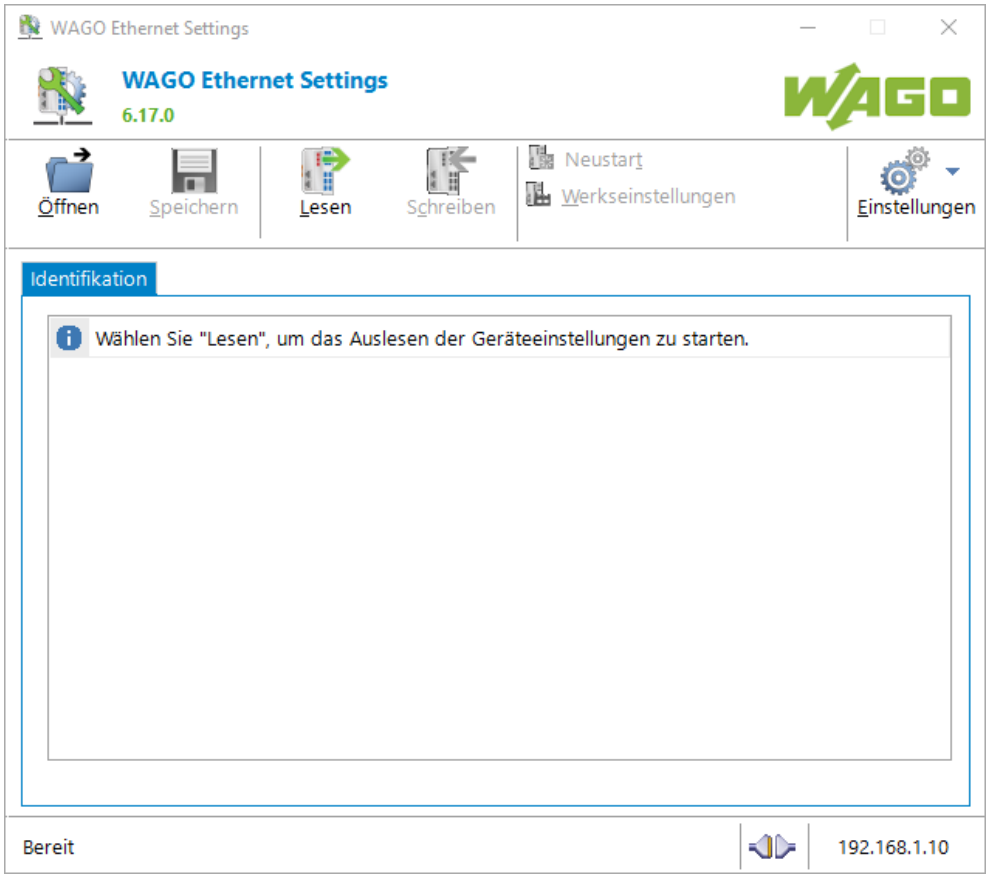



Abbildung 14: „WAGO Ethernet Settings“ – Startbildschirm (Beispiel)

5. Klicken Sie auf die Schaltfläche **[Lesen]**, um den angeschlossenen Controller einzulesen und zu identifizieren.

6. Wählen Sie das Register „Netzwerk“:

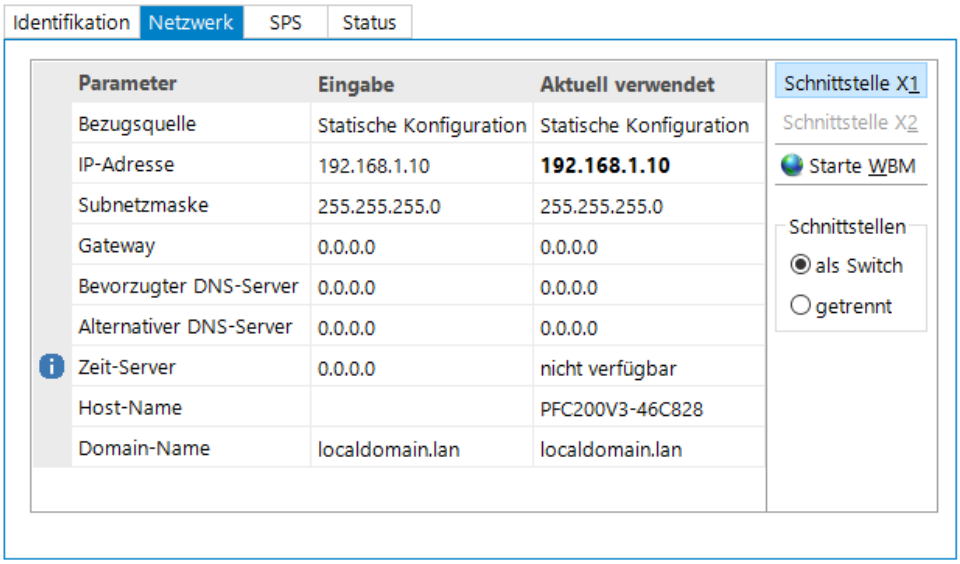



Abbildung 15: „WAGO Ethernet Settings“ – Register Netzwerk (Beispiel)

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.

### 8.3.3 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 Reset-Taster (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.

### 8.3.4 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.

### 8.3.5 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.

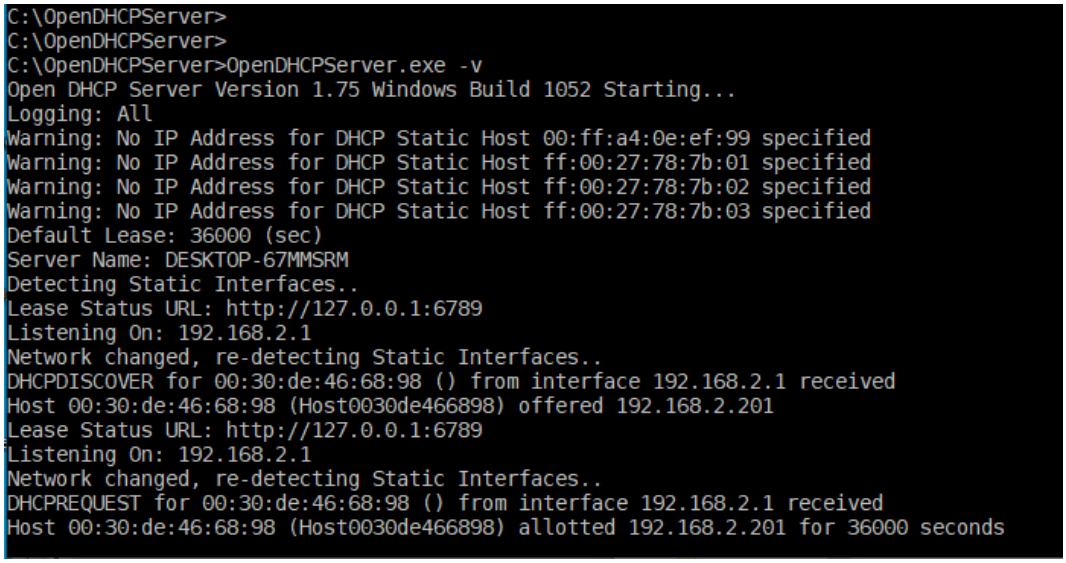



Abbildung 16: „Open DHCP, Beispielbild“

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

Der Hostname ist damit „Host0030de466898“.

## 8.4 Testen der Netzwerkverbindung

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

1. Öffnen Sie die Eingabeaufforderung.
   Geben sie dazu im Eingabefeld unter **Start** > **Ausführen…** > **Öffnen:** (Windows® XP) oder **Start** > **Programme/Dateien durchsuchen** (Windows® 7) den Befehl „cmd“ ein und bestätigen Sie die Eingabe mit der **[OK]**-Schaltfläche oder der **[Enter]**-Taste.

2. Geben Sie in der Eingabeaufforderung den Befehl „ping“ und die IP-Adresse des Controllers (z. B. `ping 192.168.1.17`) ein und bestätigen Sie die Eingabe mit der **[Enter]**-Taste.

**Hinweis**

**Host-Einträge der ARP-Tabelle zu löschen!**
Gegebenenfalls ist es sinnvoll, vor Ausführung des „pings“ die aktuellen Host-Einträge der ARP-Tabelle mit „arp -d *“ zu löschen (unter Windows® 7 als Administrator ausführen). Damit ist sichergestellt, dass kein veralteter Eintrag Grund für einen nicht erfolgreichen „ping“ ist.

3. Ihr PC sendet eine Anfrage, die vom Controller beantwortet wird. Die Antwort erscheint in der Eingabeaufforderung. Wenn die Fehlermeldung „Timeout“ erscheint, hat der Controller sich nicht ordnungsgemäß gemeldet. Überprüfen Sie bitte Ihre Netzwerkeinstellung.

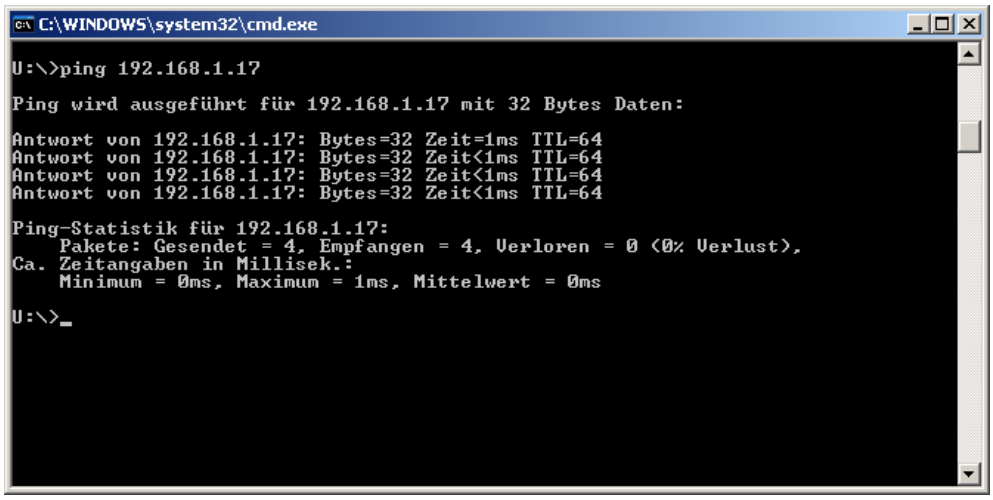



Abbildung 17: Beispiel eines Funktionstests

4. Haben Sie den Test erfolgreich durchgeführt, dann schließen Sie die Eingabeaufforderung.

# 8.5 Passwörter ändern

**Hinweis**

**Standardpasswörter ändern**
Die im Auslieferungszustand eingestellten Standardpasswörter sind in dieser Betriebsanleitung dokumentiert und bieten so keinen hinreichenden Schutz! Ändern Sie die Passwörter entsprechend Ihren Erfordernissen!

Zur Erhöhung der Sicherheit sollten Passwörter eine Mischung aus Kleinbuchstaben (a … z), Großbuchstaben (A … Z), Ziffern (0 … 9), Leerzeichen und sowie Sonderzeichen: (]!"#$%&'()*+,./:;<=>?@[\^_`{|}~-) enthalten. Allgemein bekannte Namen, Geburtsdaten und andere leicht zu erratende Informationen sollten nicht Bestandteil von Passwörtern sein.

Ändern Sie vor der Inbetriebnahme des Controllers die Standardpasswörter! Standardpasswörter sind für die Benutzergruppen „WBM-Benutzer“ und „Linux®-Benutzer“ vergeben.

Die Tabelle im Kapitel „Funktionsbeschreibung“ > ... > „Benutzer und Passwörter“ > „Gruppe WBM-Benutzer“ zeigt die Standardpasswörter für die WBM-Benutzer. Um diese Passwörter zu ändern, gehen Sie folgendermaßen vor:

1. Verbinden Sie den Controller über eine der Netzwerkschnittstellen (X1, X2) mit einem PC.
2. Starten Sie auf dem PC ein Webbrowserprogramm und rufen Sie das WBM des Controllers auf (siehe Kapitel „In Betrieb nehmen“ > … > „Konfigurieren mittels Web-Based-Management (WBM)“).
3. Melden Sie sich am Controller als Benutzer „admin“ mit dem Standardpasswort an.
4. Ändern Sie das Passwort für alle Benutzer auf der WBM-Seite „Configuration of the users for the WBM“.
5. Wählen Sie jeden Benutzer aus und geben Sie ein neues Passwort ein und bestätigen Sie dieses.

Die Tabelle im Kapitel „Funktionsbeschreibung“ > ... > „Benutzer und Passwörter“ > „Gruppe Linux®-Benutzer“ zeigt die Standardpasswörter für die Linux®-Benutzer. Um diese Passwörter zu ändern, gehen Sie folgendermaßen vor:

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

## 8.6 Ausschalten/Neustart

Um den Controller auszuschalten, schalten Sie die Versorgungsspannung ab.

Um einen Neustart des Controllers durchzuführen, betätigen Sie den Reset-Taster wie im Kapitel „Reset-Funktionen auslösen“ > „Software-Reset (Neustart)“ beschrieben.
Alternativ schalten Sie Sie den Controller aus und anschließend wieder ein.

**Hinweis**

**Neustart nach Parameteränderungen nicht durch Aus- und Wiedereinschalten hervorrufen!**
Einige Parameteränderungen erfordern einen Neustart des Controllers, um wirksam zu werden. Das Speichern der Änderungen benötigt eine gewisse Zeit.
Schalten Sie den Controller nicht aus und wieder ein, um einen Neustart auszuführen, da durch ein frühzeitiges Ausschalten Änderungen verloren gehen können.
Führen Sie einen Neustart nur durch die softwaremäßige Reboot-Funktion aus. Damit ist sichergestellt, dass alle Speichervorgänge richtig und vollständig abgeschlossen sind.

# 8.7 Reset-Funktionen auslösen

Mit dem Betriebsartenschalter und dem Reset-Taster (RST) können Sie verschiedene Reset-Funktionen auslösen.

## 8.7.1 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.

## 8.7.2 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.

## 8.7.3 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 Reset-Taster (RST) länger als 1 Sekunde aber kürzer als 8 Sekunden.

Die Ausführung wird durch ein kurzes oranges Aufleuchten aller LEDs signalisiert. Nach einigen weiteren Sekunden signalisiert die SYS-LED den erfolgreichen Bootvorgang des Controllers.

## 8.7.4 Controller-Reset

**ACHTUNG**

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

**Hinweis**

**Parameter und Passwörter werden überschrieben!**
Mit dem Controller-Reset werden Parameter und Passwörter der Linux- und WBM-Benutzer des Controllers überschrieben.
Gespeicherte Boot-Projekte einschließlich vorhandener Webvisualisierungen werden gelöscht.
Nachinstallierte Firmwarefunktionen werden nicht überschrieben.
Software-Lizenzen bleiben erhalten.
Das inaktive System wird durch den Reset nicht verändert.
Bei Rückfragen wenden Sie sich an den WAGO Support.

Nach dem Controller-Reset wird der Controller neu gestartet.

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

1. Betätigen Sie den Reset-Taster (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 (RST) zu früh loslassen, dann startet der Controller neu, ohne den Controller-Reset durchzuführen.

# 8.8 Konfigurieren

**Hinweis**

**Firmwareversion prüfen und ggf. aktualisieren!**
Prüfen Sie zu Beginn der Erstkonfiguration, ob die Firmwareversion des Controllers auf dem aktuellen Stand ist.
Die installierte Firmwareversion finden Sie auf der WBM-Seite „Status Information“.
Führen Sie ggf. ein Update auf die aktuelle Firmwareversion durch. Gehen Sie dazu wie im Kapitel „Service“ > „Firmwareänderungen“ > „Firmware-Upgrade“ beschrieben vor.

Zur Konfiguration des Controllers stehen Ihnen folgende Wege zur Verfügung:

- Zugriff über den PC mittels Webbrowser auf das Web-Based-Management (Kapitel „Konfiguration mittels Web-Based-Management (WBM)“)
- Zugriff über den PC mittels „WAGO Ethernet Settings“ (Kapitel „Konfigurieren mit ‚WAGO-Ethernet Settings‘“).

## 8.8.1 Konfigurieren mittels Web-Based-Management (WBM)

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

1. Verbinden Sie den Controller über die ETHERNET-Schnittstelle X1 und das ETHERNET-Netzwerk 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.

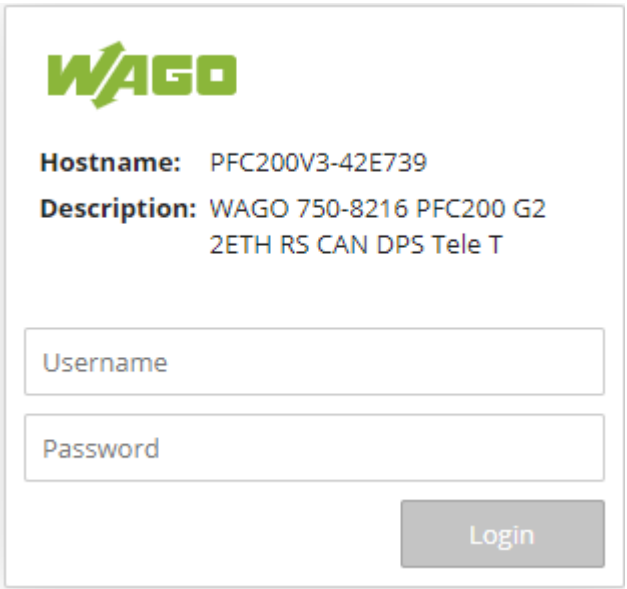



Abbildung 18: Authentifizierung eingeben (Beispiel)

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.

### 8.8.1.1 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.

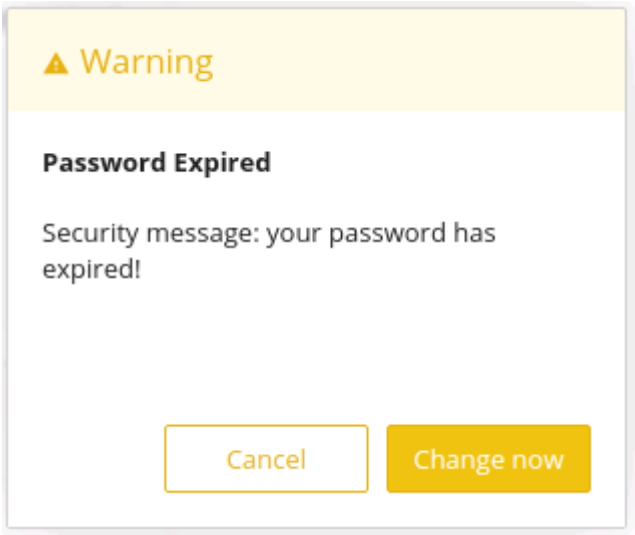



Abbildung 19: Passworterinnerung

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

Tabelle 46: 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 47: 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 | Trademarks Information | user |
| WBM Version | WBM Version Info | user |
| Configuration | | |
| PLC Runtime | PLC Runtime Configuration | user |
| Networking | | |
| TCP/IP Configuration | TCP/IP Configuration | user |
| Ethernet Configuration | Ethernet Configuration | user |
| Host/Domain Name | Configuration of Host and Domain Name | user |
| Routing | Routing | user |
| Clock | Clock Settings | user |
| Administration | | |
| Create Image | Create bootable Image | admin |
| Package Server | | |
| Firmware Backup | Firmware Backup | admin |
| Firmware Restore | Firmware Restore | admin |
| Active System | Active System | admin |
| Mass Storage | Mass Storage | admin |
| Software Uploads | Software Uploads | admin |
| Ports and Services | | |
| Network Services | Configuration of Network Services | admin |
| NTP Client | Configuration of NTP Client | admin |
| PLC Runtime Services | PLC Runtime Services | admin |
| SSH | SSH Server Settings | admin |
| Cloud Connectivity | | |
| Status | Overview | admin |

Tabelle 47: Zugriffsrechte für die WBM-Seiten

| Register/Navigation | WBM-Seitentitel | Benutzer |
|---|---|---|
| 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 |
| Docker | Docker Settings | admin |
| Users | WBM User Configuration | user |
| Fieldbus | | |
| OPC UA | OPC UA Configuration | admin |
| BACnet | | |
| Status | BACnet Status | admin |
| Configuration | BACnet Configuration | admin |
| Storage Location | BACnet Storage Location | admin |
| Files | BACnet Files | admin |
| Security | | |
| OpenVPN / IPsec | OpenVPN / IPsec Configuration | admin |
| Firewall | | |
| General Configuration | General Firewall Configuration | admin |
| Interface Configuration | Interface Configuration | admin |
| MAC Address Filter | Configuration of MAC Address Filter | admin |
| User Filter | Configuration of User Filter | admin |
| Certificates | Certificates | admin |
| Boot Mode | Boot mode configuration | admin |
| TLS | Security Settings | admin |
| Integrity | Advanced Intrusion Detection Environment (AIDE) | admin |
| WAGO Device Access | WAGO Device Access | admin |
| Diagnostic | | |
| Log Message | Log Message Viewer | user |
| Download | Download | admin |
| Network Capture | Network Capture | admin |

### 8.8.1.2 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]**.

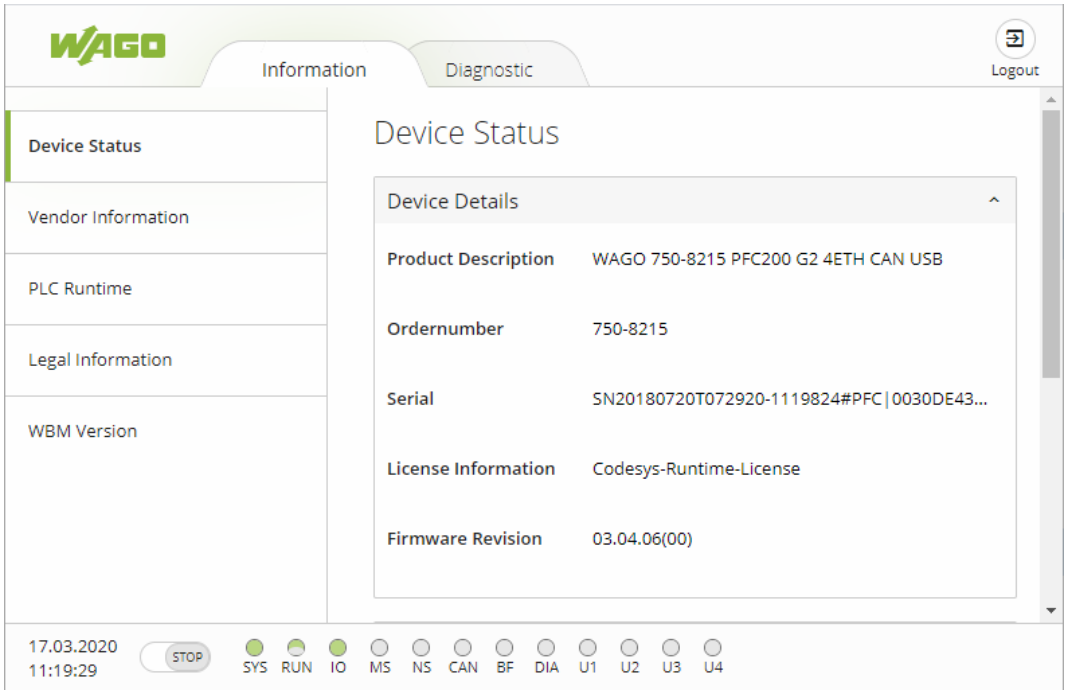



Abbildung 20: WBM-Browserfenster (Beispiel)

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.

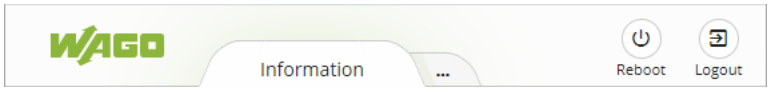



Abbildung 21: WBM-Kopfzeile mit nicht darstellbaren Registerkarten (Beispiel)

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.

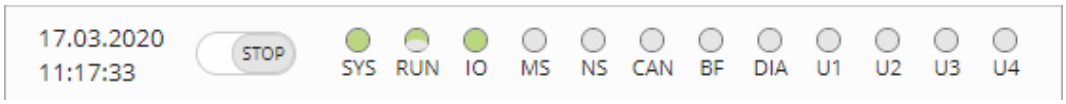



Abbildung 22: WBM-Statuszeile (Beispiel)

- 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)“.

## 8.8.2 Konfigurieren mit „WAGO Ethernet Settings“

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

**Hinweis**

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

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

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

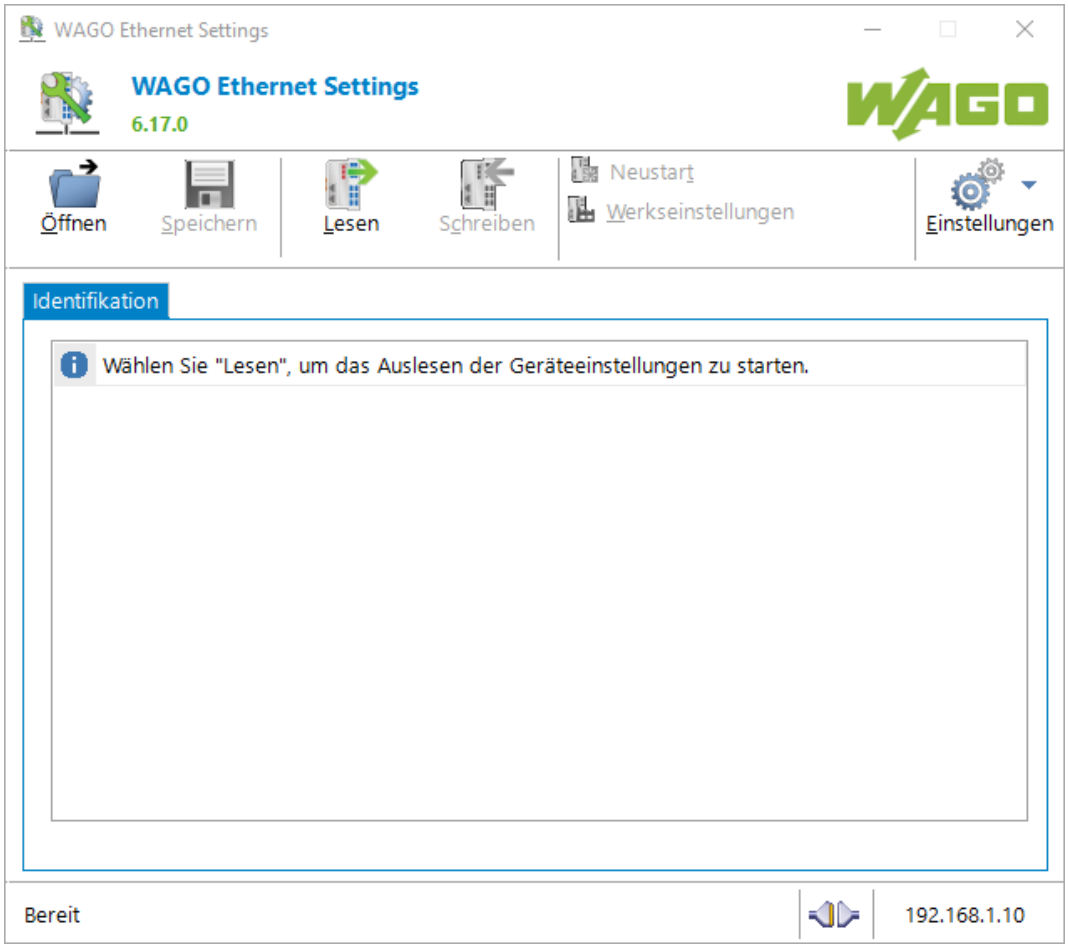



Abbildung 23: „WAGO Ethernet Settings“ – Startbildschirm (Beispiel)

Klicken Sie hierzu auf „Einstellungen“ und dann auf „Kommunikation“.

Im nun neu geöffneten Fenster „Kommunikationseinstellungen“ nehmen Sie die Einstellungen entsprechend Ihren Erfordernissen vor.

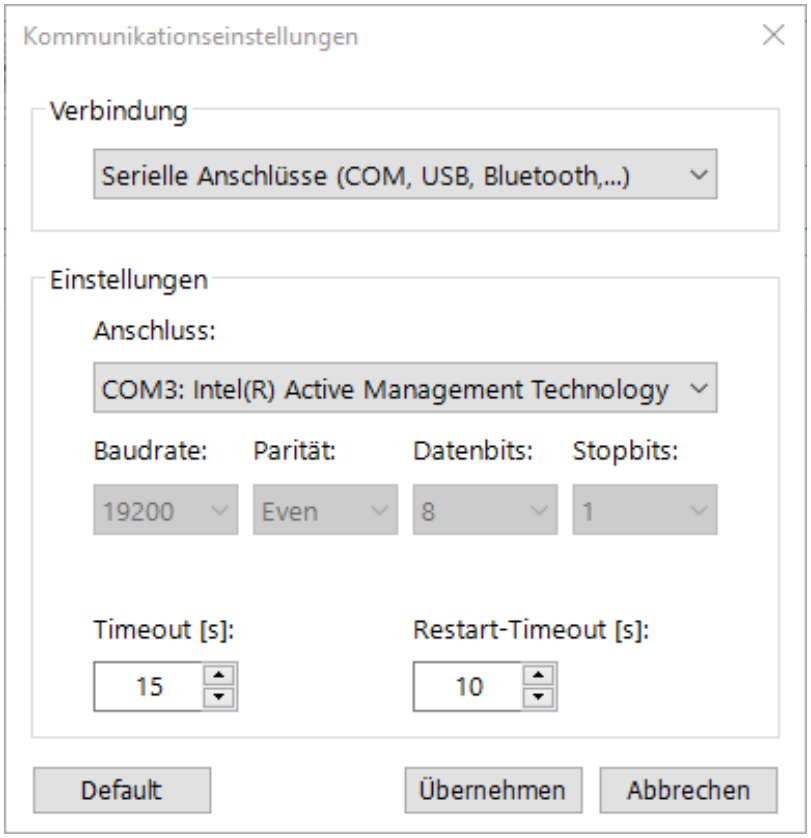



Abbildung 24: „WAGO Ethernet Settings“ – Kommunikationsverbindung (Beispiel)

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

Wurde „WAGO Ethernet Settings“ mit den korrekten Parametern bereits gestartet, ist es möglich, durch Klicken auf **[Lesen]** die Verbindung zum Controller aufzubauen.

#### 8.8.2.1 Registerkarte Identifikation

Hier finden Sie einen Überblick über das angeschlossene Gerät.

Neben einigen festen Werten wie Artikelnummer, MAC-Adresse und Firmware-Version ist auch die aktuell verwendete IP-Adresse und die Art, wie sie konfiguriert wurde, ersichtlich.

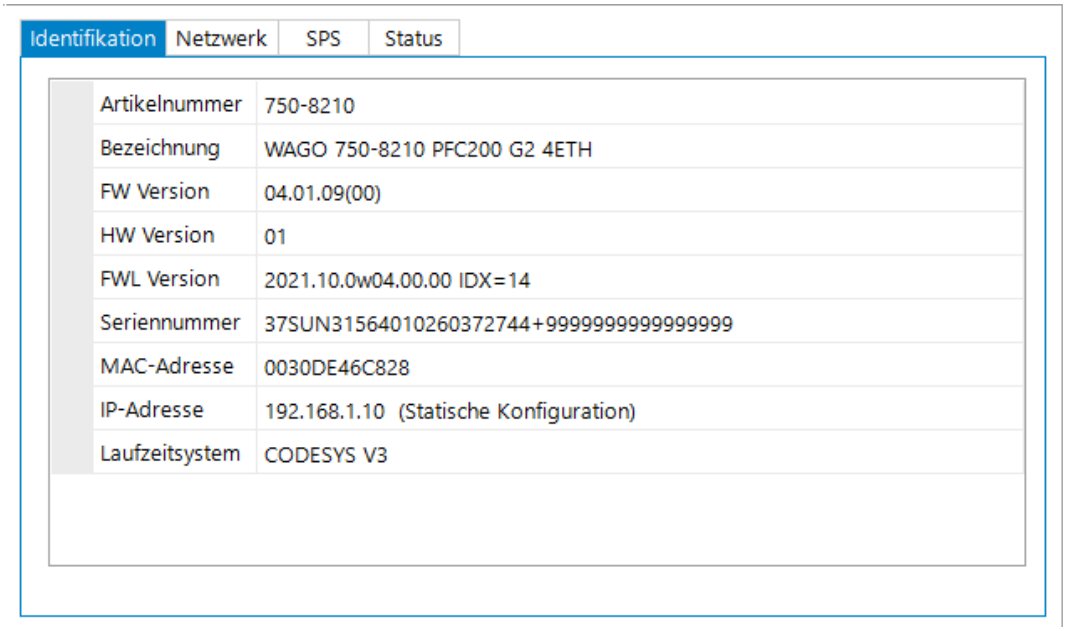



Abbildung 25: „WAGO Ethernet Settings“ – Registerkarte Identifikation (Beispiel)

### 8.8.2.2 Registerkarte Netzwerk

Dieser Reiter wird verwendet um die Netzwerkeinstellungen zu konfigurieren.

In der Spalte „Eingabe“ können Werte verändert werden und in der Spalte „Aktuell Verwendet“ sind die aktuell tatsächlich verwendeten Parameter zu sehen.

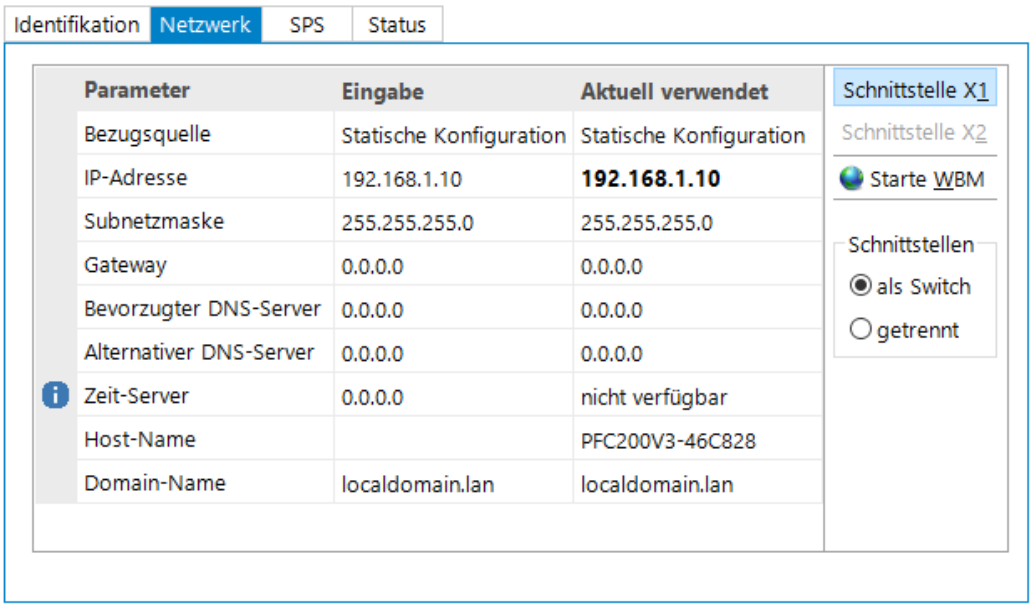



Abbildung 26: „WAGO Ethernet Settings“ – Registerkarte Netzwerk (Beispiel)

**Bezugsquelle**
Wählen Sie hier aus, wie der Controller seine IP-Adresse ermitteln soll: Statisch, per DHCP oder per BootP.

**IP-Adresse, Subnetzmaske, Gateway**
Geben Sie hier im Falle der statischen Konfiguration die jeweiligen Netzwerkparameter ein.

**Hinweis**

**Eingeschränkte Einstellung für Default-Gateways!**
Mit „WAGO Ethernet Settings“ kann nur das Default-Gateway 1 eingestellt werden.
Das Default-Gateway 2 kann ausschließlich im WBM eingestellt werden!

**Bevorzugter DNS-Server, Alternativer DNS-Server**
Geben Sie hier bei Bedarf die IP-Adresse eines erreichbaren DNS Servers für die Auflösung von Netzwerknamen ein.

**Zeit-Server**
Geben Sie hier die IP-Adresse eines Zeitservers ein wenn der Controller seine Systemzeit über NTP einstellen soll.

**Host-Name**
Hier wird der Hostname des Controller angezeigt. Im Auslieferungszustand wird

der Hostaname zusammengesetzt aus dem String „CC100-“ und den letzten 3 Byte der MAC-Adresse.
Dieser Standardwert wird ebenfalls immer dann verwendet, wenn der selbstgewählte Name in der Spalte „Eingabe“ gelöscht wird.

**Domain-Name**
Hier wird der aktuelle Domain-Name angezeigt. Diese Einstellung kann bei dynamischen Konfigurationen z. B. DHCP automatisch überschrieben werden.

### 8.8.2.3 Registerkarte SPS

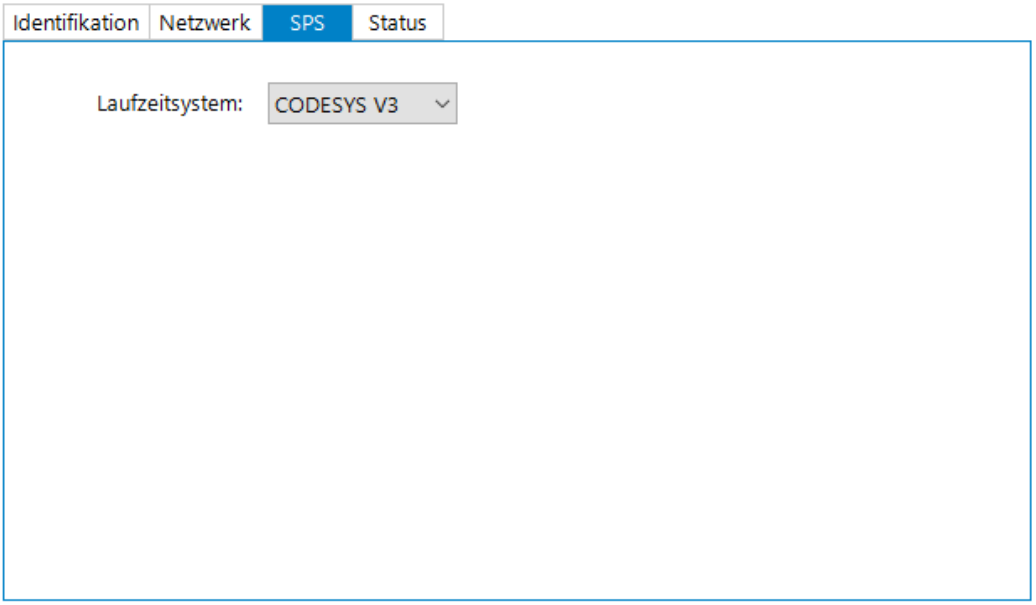



Abbildung 27: „WAGO Ethernet Settings“ – Registerkarte Protokoll (Beispiel)

Hier können Sie das Laufzeitsystem auswählen.

### 8.8.2.4 Registerkarte Status

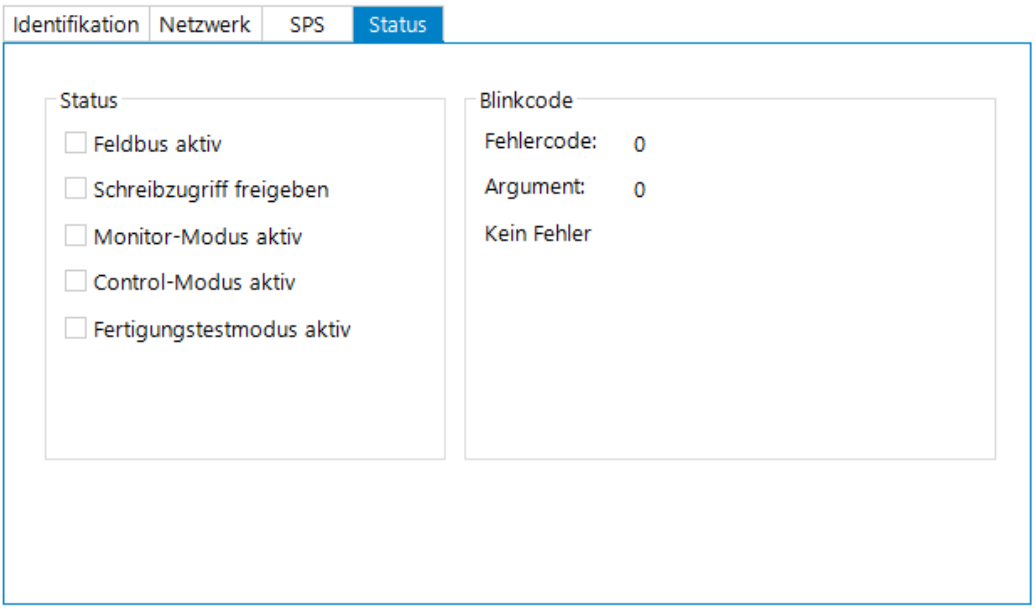



Abbildung 28: „WAGO Ethernet Settings“ – Registerkarte Status (Beispiel)

Hier werden allgemeine Informationen über den Status des Controllers angezeigt.

# 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 48: 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)<br>PROFIBUS (-49 … -45)<br>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…]).

# 9.4 Prozessabbild

## 9.4.1 Analoge Eingänge

Die analogen Eingänge AI1 und AI2 werden pro Kanal über den Datentyp WORD (16 Bit) dargestellt.

Tabelle 49: Prozessabbild analoge Eingänge

| Kanal | Pin | Daten-typ | Mess-wert | Wertebereich | | |
|---|---|---|---|---|---|---|
| | | | | Hex. | Dez. | Bin. |
| AI1 | X14.1 | WORD | < 0 V | 0x0000 | 0 | 0000.0000. 0000.0000 |
| | | | 0 … 10 V | 0x0000 … 0x7FF8 | 0 … 32760 | 0000.0000. 0000.0000 … 0111.1111. 1111.1000 |
| AI2 | X14.3 | | > 10 V | 0x7FFB | 32763 | 0111.1111. 1111.1011 |

## 9.4.2 Analoge Ausgänge

Die analogen Ausgänge AO1 und AO2 werden pro Kanal über den Datentyp WORD (16 Bit) dargestellt.

Tabelle 50: Prozessabbild analoge Ausgänge

| Kanal | Pin | Daten-typ | Mess-wert | Wertebereich | | |
|---|---|---|---|---|---|---|
| | | | | Hex. | Dez. | Bin. |
| AO1 | X6.1 | WORD | 0 … 10 V | 0x0000 … 0x7FFF | 0 … 32767 | 0000.0000. 0000.0000 … 0111.1111. 1111.1111 |
| AO2 | X6.3 | | | | | |

### 9.4.3 Analoge Temperatureingänge

Die analogen Temperaturfühlereingänge PT1+ / PT1– und PT2+ / PT2– werden mit einer Auflösung von 1 Digit pro 0,1 °C über den Datentyp INT (16 Bit) dargestellt.

Tabelle 51: Prozessabbild analoge Temperatureingänge

| Kanal | Pin | Daten-typ | Mess-wert | Wertebereich | | |
|---|---|---|---|---|---|---|
| | | | | Hex. | Dez. | Bin. |
| PT1+ / PT1– | X13.1 / X13.2 | INT | < – 60 °C | 0x8001 | –32767 | 1.000.000. 000.000.000 |
| | | | –60 °C … 350 °C | 0xFDA8* … 0x0DAC | –600 … 3500 | 1111.1101. 1010.1000* … 0000.1101. 1010.1100 |
| PT2+ / PT2– | X13.3 / X13.4 | | > 350 °C | 0x0DAC | 3500 | 0000.1101. 1010.1100 |

*Temperaturwerte unter 0 °C werden binär und hexadezimal im Zweierkomplement dargestellt.

### 9.4.4 Digitale Eingänge

Die digitalen Eingänge DI1 … DI8 werden pro Kanal über den Datentyp BOOL dargestellt. Zusätzlich werden die digitalen Eingänge über den Datentyp BYTE dargestellt.

Tabelle 52: Prozessabbild digitale Eingänge

| Kanal | Pin | Daten-typ | Mess-wert | Wertebereich | | |
|---|---|---|---|---|---|---|
| | | | | Hex. | Dez. | Bin. |
| DI [1 … 8] | X12 | BYTE | 0 / +24 V DC | 0x00 … 0xFF | 0 … 255 | 0000.0000 … 1111.1111 |
| DI1 | X12.3 | BOOL | | – | – | TRUE / FALSE |
| DI2 | X12.4 | | | | | |
| DI3 | X12.5 | | | | | |
| DI4 | X12.6 | | | | | |
| DI5 | X12.7 | | | | | |
| DI6 | X12.8 | | | | | |
| DI7 | X12.9 | | | | | |
| DI8 | X12.10 | | | | | |

### 9.4.5 Digitale Ausgänge

Die digitalen Ausgänge DO1 … DO4 werden pro Kanal über den Datentyp BOOL dargestellt. Zusätzlich werden die digitalen Ausgänge über den Datentyp BYTE dargestellt.

Tabelle 53: Prozessabbild digitale Ausgänge

| Kanal | Pin | Daten-typ | Mess-wert | Wertebereich | | |
|---|---|---|---|---|---|---|
| | | | | Hex. | Dez. | Bin. |
| DI [1 … 8] | X5 | BYTE | 0 / +24 V DC | 0x00 … 0x0F | 0 … 15 | 0000.0000 … 0000.1111 |
| DO1 | X5.3 | BOOL | | – | – | TRUE / FALSE |
| DO2 | X5.5 | | | | | |
| DO3 | X5.7 | | | | | |
| DO4 | X5.9 | | | | | |

# 10 Diagnose

## 10.1 Betriebs- und Statusmeldungen

In den nachfolgenden Tabellen werden alle Betriebs- und Statusmeldungen des Controllers beschrieben, die durch die LEDs angezeigt werden.

### 10.1.1 LEDs System

#### 10.1.1.1 LED „SYS“

Tabelle 54: Diagnose LED „SYS“

| Status | Bedeutung | Abhilfe |
|---|---|---|
| Grün | Betriebsbereit - Systemstart wurde ohne Fehler beendet | --- |
| Orange | Gerät befindet sich im Anlauf/Boot-Vorgang und der RST-Taster ist nicht gedrückt. | --- |
| Orange blinkend | „Fix IP Address“-Modus, temporäre Einstellung bis zum nächsten Neustart | Verbinden Sie sich über die Standardadresse (192.168.1.17) mit dem Gerät oder starten Sie das Gerät neu, um den ursprünglich eingestellten Wert wiederherzustellen. |
| Grün/rot blinkend | Firmware-Update-Modus | --- |

#### 10.1.1.2 LED „RUN“

Tabelle 55: Diagnose LED „RUN“

| Status | Bedeutung | Abhilfe |
|---|---|---|
| Grün | Applikationen geladen und alle im Status „RUN“ | --- |
| Grün blinkend | Keine Applikation und kein Boot-Projekt geladen | Laden Sie eine Applikation oder ein Boot-Projekt. |
| Rot | Applikationen geladen und alle im Status „STOP“ | Stellen Sie den Betriebsartenschalter auf „RUN“, um die Applikation zu starten. |
| Grün/rot blinkend | Mindestens jeweils eine Applikation im Status „RUN“ und im Status „STOP“ | Starten Sie die gestoppte Applikation. |

Tabelle 55: Diagnose LED „RUN“

| Status | Bedeutung | Abhilfe |
|---|---|---|
| Rot, einmal kurz verlöschend | Warmstart-Reset durchgeführt | --- |
| Rot, einmal länger verlöschend | Kaltstart-Reset durchgeführt | --- |
| Rot blinkend | Mindestens eine Applikation nach Exception (z. B. Speicherzugriffs-fehler) im Status „STOP“ | Starten Sie die Applikation durch einen Reset mit dem Betriebsartenschalter oder in der verbundenen IDE neu. Kann die Applikation nicht gestartet werden, starten Sie den Controller neu. Tritt der Fehler wieder auf, wenden Sie sich an den WAGO Support. |
| Orange/grün blinkend | Auslastung oberhalb des Schwellwerts 1 | Versuchen Sie, das System zu entlasten:<br>- Ändern Sie das CODESYS Programm.<br>- Beenden Sie nicht benötigte Feldbuskommunikationen oder konfigurieren Sie Feldbusse um.<br>- Entfernen Sie eventuell unkritische Tasks aus dem RT-Bereich.<br>- Wählen Sie eine größere Zykluszeit für IEC-Tasks. |
| Orange | Laufzeitsystem im Debug-Zustand (Breakpoint, Einzelschritt, Einzelzyklus) | Setzen Sie die Applikation in der verbundenen IDE mit Einzelschritt oder Start fort.<br>Entfernen Sie ggf. Breakpoints.<br>Wurde die Verbindung unterbrochen, stellen Sie den Betriebsartenschalter auf „STOP“ und anschließend wieder auf „RUN“, um die Applikation weiterlaufen zu lassen. |
| Aus | Kein Laufzeitsystem geladen | Aktivieren Sie ein Laufzeitsystem, z. B. über das WBM. |

## 10.1.2 LED Netzwerkanschluss

### 10.1.2.1 LED „LNK ACT“

Die LED „LNK ACT“ zeigt folgende Diagnosen an:

Tabelle 56: Diagnose LED „LNK ACT“

| Status | Bedeutung | Abhilfe |
|---|---|---|
| Aus | Keine Netzwerk-Kommunikation | Prüfen Sie ggf. die Netzwerkverbindungen und Netzwerkeinstellungen. |
| Grün | Verbindung zum physikalischen Netzwerk vorhanden | --- |
| Grün blinkend | Netzwerk-Kommunikation findet statt | --- |

### 10.1.3 LED Speicherkartensteckplatz

Die LED für den Speicherkartensteckplatz zeigt folgende Diagnosen an:

Tabelle 57: Diagnose LED Speicherkartensteckplatz

| Status | Bedeutung | Abhilfe |
|---|---|---|
| Aus | Kein Schreib- oder Lesezugriff auf Speicherkarte | --- |
| Orange leuchtend | Schreib- oder Lesezugriff auf Speicherkarte | --- |
| Orange blinkend | | |

# 11 Service

## 11.1 Speicherkarte einfügen und entfernen

### 11.1.1 Speicherkarte einfügen

1. Öffnen Sie mit Hilfe eines Betätigungswerkzeuges oder eines Schraubendrehers die transparente Abdeckklappe, indem Sie diese nach oben klappen. Die Ansatzstelle für das Werkzeug ist mit einem Pfeil gekennzeichnet.

2. Nehmen Sie die Speicherkarte so, dass die Kontakte sichtbar auf der rechten Seite sind und die schräge Kante oben ist, wie in der nachfolgenden Abbildung dargestellt.

3. Fügen Sie die Speicherkarte dann in dieser Position in den dafür vorgesehenen Steckplatz ein.

4. Schieben Sie die Speicherkarte ganz ein. Wenn Sie sie loslassen, wird die Speicherkarte durch Federkraft wieder etwas herausgeschoben und rastet dann ein (Push-Push-Mechanismus).

5. Schließen Sie die Abdeckklappe, indem Sie diese wieder nach unten klappen, bis sie einrastet.

6. Durch die Bohrung im Gehäuse neben der Klappe und in der Klappe haben Sie die Möglichkeit, die geschlossene Klappe zu verplomben.

### 11.1.2 Speicherkarte entfernen

1. Entfernen Sie eine gegebenenfalls vorhandene Plombe.

2. Öffnen Sie mit Hilfe eines Betätigungswerkzeuges oder eines Schraubendrehers die transparente Abdeckklappe, indem Sie diese nach oben klappen. Die Ansatzstelle für das Werkzeug ist mit einem Pfeil gekennzeichnet.

3. Um die Speicherkarte zu entnehmen, müssen Sie diese zunächst etwas in den Steckplatz hineindrücken (Push-Push-Mechanismus). Dabei wird die mechanische Verriegelung gelöst.

4. Sobald Sie die Speicherkarte wieder loslassen, wird sie durch Federkraft etwas herausgeschoben.

5. Entnehmen Sie die Speicherkarte.

6. Schließen Sie die Abdeckklappe, indem Sie diese wieder nach unten klappen, bis sie einrastet.

## 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.

**Hinweis**

**Firmwareversion beachten!**
Das Produkt ist kompatibel ab Firmware 19.
Ein Downgrade auf eine Version ≤ Firmware 19 ist nicht zulässig.

Sie können die Firmware auf folgende Arten aktualisieren:

- mit WAGOupload
- mit Speicherkarte und WBM

## 11.2.1 Firmware-Update/-Downgrade mit WAGOupload durchführen

**Hinweis**

**WAGOupload-Version beachten!**
Das Produkt ist kompatibel ab der WAGOupload-Version 1.14.0.0.

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.

## 11.3 Root-Zertifikate aktualisieren

Wenn Sie die Root-Zertifikate auf dem Controller aktualisieren möchten, gehen Sie folgendermaßen vor:

1. Laden Sie das aktuelle Root-CA-Bundle von der Webseite https://curl.haxx.se/ca auf Ihren PC herunter.

2. Benennen Sie die Datei um nach „ca-certificates.crt“.

3. Übertragen Sie die Datei mit einem SFTP- oder FTP-Client auf den Controller in das Verzeichnis /etc/ssl/certs.

4. Starten Sie den Controller neu. Nutzen Sie dazu die Reboot-Funktion im WBM.

# 12 Demontieren

## 12.1 Geräte entfernen

**GEFAHR**

**Nicht an Geräten unter Spannung arbeiten!**
Gefährliche elektrische Spannung kann zu elektrischem Schlag und Verbrennungen führen.
Schalten Sie immer alle verwendeten Spannungsversorgungen für das Gerät ab, bevor Sie das Gerät montieren, installieren, Störungen beheben oder Wartungsarbeiten vornehmen.

### 12.1.1 Controller entfernen

Hebeln Sie die orangefarbene Rastfußentriegelung mit einem Werkzeug heraus, bis die Rastfußentriegelung mit einem Klick einrastet.

Die Rastfußentriegelung bleibt nach dem Einrasten in dieser herausgehebelten Stellung. Die Rastfußentriegelung springt nicht wieder in das Gehäuse zurück.

Sie können den Controller nun senkrecht nach oben von der Tragschiene abheben und entfernen.

Die Rastfußentriegelung springt automatisch zurück in das Gehäuse, sobald der Controller von der Tragschiene gelöst ist.

# 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

## 14.1 Werkzeuge

Setzen Sie nur isoliertes Werkzeug ein.

Tabelle 58: Zubehör – Werkzeuge

| | | |
|---|---|---|
| Entriegelungswerkzeug *picoMAX*® | | 2092-1630 |
| Betätigungswerkzeug, mit teilisoliertem Schaft | Typ 1,<br>Klinge<br>2,5 mm × 0,4 mm | 210-719 |

# 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 59: 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 60: WBM-Seite „Device Status“ – Gruppe „Network TCP/IP Details“

| Parameter | Bedeutung | |
|---|---|---|
| Bridge <n> | Aktuell konfigurierte Bridge;<br>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;<br>dies tritt z. B. auf, wenn durch Änderungen an der Bridge-Konfiguration eine Bridge hinzugefügt wurde.<br>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;<br>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 61: WBM-Seite „PLC Runtime Information” – Gruppe „Runtime“

| Parameter | Bedeutung |
|---|---|
| Version | Hier wird die Version des aktivierten Laufzeitsystems angezeigt.<br>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 62: 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 63: 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 64: 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;<br>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 65: WBM-Seite „TCP/IP Configuration“ – Gruppe „DNS Server“

| Parameter | Bedeutung |
|---|---|
| Active | Hier werden die aktiven DNS-Server angezeigt.<br>Es können bis zu 3 aktive DNS-Server genutzt werden.<br>Der Index spiegelt die Anfrage-Reihenfolge wider.<br>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.<br>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.<br>Wenn kein DNS-Server eingetragen wurde, erscheint die Anzeige „no DNS Servers configured“. |
| New Server IP | Hier fügen Sie weitere DNS-Serveradressen hinzu.<br>Sie können maximal 3 Adressen eintragen.<br>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 66: 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.<br>Klicken Sie dazu auf die entsprechende Optionsschaltfläche. Die Zuordnung wird farblich markiert.<br>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 67: 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 68: 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 69: 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;<br>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 70: 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.<br>Die Auswahlliste wird geräte- und interface-abhängig generiert.<br>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 71: 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 72: 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 73: 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.<br>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.<br>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 74: 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.<br>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.<br>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.<br>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.<br>Der kleinste Wert ist 0.<br>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.<br>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 75: 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 76: 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 „Clock Settings“

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

**Gruppe „Timezone and Format“**

Tabelle 77: 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 78: 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 79: 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.

### 15.1.1.2.7 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 80: 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.

### 15.1.1.2.8 Seite „Firmware Backup“

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

#### Gruppe „Firmware Backup“

Tabelle 81: 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 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]**.

### 15.1.1.2.9 Seite „Firmware Restore“

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

#### Gruppe „Firmware Restore“

Tabelle 82: 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.<br>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.<br>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.<br>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.<br>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.<br>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]**.

### 15.1.1.2.10 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 83: 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 84: 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!

#### 15.1.1.2.11 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 85: 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 86: 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]**.

#### 15.1.1.2.12 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 87: 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.<br>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.

#### 15.1.1.2.13 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 88: 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 89: 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 90: 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 91: 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 92: 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.

#### 15.1.1.2.14 Seite „Configuration of NTP Client“

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

**Gruppe „NTP Client Configuration“**

Tabelle 93: 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.<br>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.

#### 15.1.1.2.15 Seite „PLC Runtime Services“

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

**Gruppe „CODESYS V3“**

Tabelle 94: 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.

#### 15.1.1.2.16 Seite „SSH Server Settings“

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

**Gruppe „SSH Server“**

Tabelle 95: 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.

#### 15.1.1.2.17 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 96: 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.

#### 15.1.1.2.18 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 97: 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.<br>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.<br>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.<br>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.<br>Amazon Web Services (AWS) verwendet immer TLS. |

Tabelle 97: 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.<br>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.<br>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.<br>Dieses Auswahlfeld ist nur aktiv, wenn eine korrekt formatierte SD-Karte gesteckt ist.<br>(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 97: 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.<br>(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.<br>(Weitere Informationen finden Sie im Anwendungshinweis A500920.) |
| Standard commands | Hier stellen Sie ein, ob die integrierten Standardkommandos unterstützt werden sollen.<br>(Die Liste der Standardkommandos finden Sie im Anwendungshinweis A500920.)<br>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.<br>Dieser Parameter ist optional, d. h., wenn das Feld leer gelassen wird, wird dieses Property nicht mitgesendet.<br>Zur Erstellung dieses Properties stehen die folgenden Platzhalter zur Verfügung:<br>• <m>: Nachrichtentype<br>• <p>: Protokoll-Version<br>• <d>: DeviceId<br>Beispiele:<br>• MyKey=HelloWorld_<m><br>• TestKey=<m>/<p>/<d><br>• 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 98: Anzeige der Auswahl- und Eingabefelder abhängig von der ausgewählten Cloud-Plattform

| Auswahl- oder Eingabefeld | Cloud-Plattform | | | | | | |
|---|---|---|---|---|---|---|---|
| | WAGO Cloud | Azure | MQTT AnyCloud | IBM Cloud | Amazon Web Services | SAP IoT Services | Azure Device Provisioning Service (DPS) |
| Enabled | X | X | X | X | X | X | X |
| Cloud platform | X | X | X | X | X | X | X |
| Hostname | X | X | X | X | X | X | |
| Port number | | | X | X | (X) | X | |
| Device ID | X | X | | | | | |
| Client ID | | | X | X | X | X | |
| Authentication | | X | | | | | X |
| Activation Key | X | X2 | | | | | X2 |
| Clean Session | | | X | (X) | (X) | X | |
| TLS | | | X | X | (X) | X | |
| CA file | | X | X | X | X | X | X |
| User | | | X | X | | | |
| Password | | | X | 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) | X |
| Use compression | X | X1 | X1 | | | | X1 |
| Cache mode | X | X | X | X | X | X | X |
| Last Will | | | X | X | X | X | |
| Last Will Topic | | | X3 | X3 | X3 | X3 | |
| Last Will Message | | | X3 | X3 | X3 | X3 | |
| Last Will QoS | | | X3 | X3 | X3 | X3 | |
| Last Will Retain | | | X3 | X3 | (X3) | X3 | |
| Device info | | X1 | X1 | X1 | X1 | | X1 |
| Device status | | X1 | X1 | X1 | X1 | | X1 |

Tabelle 98: Anzeige der Auswahl- und Eingabefelder abhängig von der ausgewählten Cloud-Plattform

| Auswahl- oder Eingabefeld | Cloud-Plattform | | | | | | |
|---|---|---|---|---|---|---|---|
| | WAGO Cloud | Azure | MQTT AnyCloud | IBM Cloud | 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 99: Auswahlmöglichkeit des Datenprotokolls abhängig von der ausgewählten Cloud-Plattform

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

X: Auswahl möglich
(X): Fest eingestellt

Tabelle 100: 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 101: 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 102: 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

#### 15.1.1.2.19 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 103: 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]**.

#### 15.1.1.2.20 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 104: 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.<br>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.).<br>Der Community-Name darf maximal 32 Zeichen lang sein und keine Leerzeichen enthalten.<br>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.<br>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 105: 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.).<br>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.<br>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]**.

#### 15.1.1.2.21 Seite „Configuration of SNMP v3 Parameters“

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

**Gruppe „Users“**

Tabelle 106: 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.<br>Mögliche Werte sind:<br>- Keine Authentifizierung benutzen („None“)<br>- Message Digest 5 („MD5“)<br>- 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.<br>Mögliche Werte sind:<br>- Keine Verschlüsselung („None“)<br>- Data Encryption Standard („DES“)<br>- 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.<br>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 106: WBM-Seite „Configuration of SNMP v3 Parameters“ – Gruppe „Users“

| Parameter | Bedeutung |
|---|---|
| Authentication Type | Hier geben Sie den Authentifizierungstyp für die SNMP-v3-Pakete ein.<br>Mögliche Werte sind:<br>- Keine Authentifizierung benutzen („None“)<br>- Message Digest 5 („MD5“)<br>- 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.<br>Mögliche Werte sind:<br>- Keine Verschlüsselung („None“)<br>- Data Encryption Standard („DES“)<br>- 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.<br>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 107: 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.<br>Mögliche Werte sind:<br>- Keine Authentifizierung benutzen („None“)<br>- Message Digest 5 („MD5“)<br>- 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.<br>Mögliche Werte sind:<br>- Keine Verschlüsselung („None“)<br>- Data Encryption Standard („DES“)<br>- 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.<br>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 107: 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.<br>Mögliche Werte sind:<br>- Keine Authentifizierung benutzen („None“)<br>- Message Digest 5 („MD5“)<br>- 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.<br>Mögliche Werte sind:<br>- Keine Verschlüsselung („None“)<br>- Data Encryption Standard („DES“)<br>- 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]**.

#### 15.1.1.2.22 Seite „Docker Settings“

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

**Gruppe „Docker Status“**

Tabelle 108: 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.

### 15.1.1.2.23 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 109: 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.<br>Zulässige Zeichen für das Passwort sind folgende ASCII-Zeichen:<br>a … z, A … Z, 0 … 9,<br>und die Sonderzeichen:<br>!"#$%&'()*+,./:;<=>?@[]^_`{}\|~-. |
| 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 110: 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.<br>Folgende Werte sind einstellbar:<br>Error / Warning / Info / Debug.<br>Mit dem Log-Level „Error“ werden nur Fehlermeldungen ausgegeben, mit dem Log-Level „Info“ auch Statusmeldungen.<br>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 111: WBM-Seite „OPC UA Configuration“ – Gruppe „OPC UA Server Security Settings“

| Parameter | Bedeutung |
|---|---|
| Anonymous Access | Anonymen Zugriff auf den Server zulassen<br>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<br>Je nach Auswahl der Betriebsart stehen Ihnen verschiedene OPC UA Endpoints zum Verbindungsaufbau zu Verfügung:<br>None:<br>Lediglich der OPC UA Endpoint **None** wird aktiviert. Dieser ermöglicht eine ungesicherte Verbindung zum OPC UA Server.<br>None + Sign + SignAndEncrypt:<br>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.<br>Sign + SignAndEncrypt:<br>Die Endpoints **Sign** sowie **SignAndEncrypt** stehen zur Verfügung.<br>SignAndEncrypt:<br>Lediglich der Endpoint **SignAndEncrypt** steht zur Verfügung. |
| Security Policies | Auswahl der Security Policies<br>Hierüber wird die Verschlüsselungsstärke des OPC UA Servers eingestellt. Zur Auswahl stehen dabei:<br>Aes128Sha256RsaOaep and better,<br>Basic256Sha256 and better,<br>Aes256Sha256RsaPss. |

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

#### 15.1.1.3.2 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 112: WBM-Seite „BACnet Status” – Gruppe „BACnet Information“

| Parameter | Bedeutung |
|---|---|
| State | Hier wird angezeigt, ob der Feldbus BACnet aktiviert (enabled) oder deaktiviert (disabled) ist. |
| 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 113: WBM-Seite „BACnet Status” – Gruppe „BACnet License“

| Parameter | Bedeutung |
|---|---|
| Type | Hier wird der Typ der Lizenz angezeigt. |
| User Objects | Hier wird die Anzahl der mit der Lizenz möglichen BACnet-Objekte angezeigt. |

#### 15.1.1.3.3 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. Um die Runtime neu zu starten, nutzen Sie die Schaltfläche **[Restart]**. Schalten Sie den Controller nicht zu früh aus!

**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 der Runtime erfolgt zur Sicherheit eine Abfrage über ein Pop-Up-Fenster, ob der Neustart gewünscht ist.

Tabelle 114: WBM-Seite „BACnet Configuration” – Gruppe „BACnet Service“

| Parameter | Bedeutung |
|---|---|
| Service active | Hier aktivieren/deaktivieren Sie den Feldbus BACnet. |
| Runtime restart<br><br>**[Restart]** | Mit dieser Schaltfläche führen Sie einen Neustart der Runtime durch. |

**Gruppe „BACnet Settings“**

Diese Gruppe beinhaltet Basiseinstellungen für den Feldbus.

Tabelle 115: WBM-Seite „BACnet Configuration” – Gruppe „BACnet Settings“

| Parameter | Bedeutung |
|---|---|
| Port number | Hier stellen Sie den Port für die BACnet-Kommunikation des Feldbusses ein. |
| 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). |

### Gruppe „BACnet Data Reset“

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

Tabelle 116: 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. |

### 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 117: WBM-Seite „BACnet Storage Location” – Gruppe „BACnet Persistence“

| Parameter | Bedeutung | |
|---|---|---|
| Storage location | Hier wählen Sie den Speicherort für die Persistenzdaten aus.<br>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.<br>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 118: WBM-Seite „BACnet Storage Location” – Gruppe „BACnet Trendlog“

| Parameter | Bedeutung | |
|---|---|---|
| Storage location | Hier wählen Sie den Speicherort für die Trendlogdaten aus.<br>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.<br>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 119: WBM-Seite „BACnet Storage Location” – Gruppe „BACnet Eventlog“

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

### 15.1.1.3.5 Seite „BACnet Files“

Auf dieser Seite können Sie eine Override-Datei im Controller austauschen.

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!

#### Gruppe „BACnet override.xml“

Tabelle 120: WBM-Seite „BACnet Files” – Gruppe „BACnet override.xml“

| Parameter | Bedeutung |
|---|---|
| Choose file… | Hier wählen Sie die gewünschte Datei auf dem Controller oder PC aus. |
| **[Upload]** | Mit dieser Schaltfläche übertragen Sie die ausgewählte Datei vom PC zum Controller. |

### 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 121: 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 122: 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 123: 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.<br>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 124: 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.<br>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.<br>Die Eingabe ist nur bei deaktiviertem „ICMP echo protection“-Schutz wirksam.<br>„0“ = „Disabled“ |
| ICMP burst limit<br>(0 = disabled) | Hier geben Sie die maximale Anzahl „ICMP echo burst“ pro Sekunde an.<br>Die Eingabe ist nur bei deaktiviertem „ICMP echo protection“-Schutz wirksam.<br>„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.

Auf Controllern mit Telecontrol-Funktionalität werden standardmäßig die in der nachfolgenden Tabelle aufgelisteten Firewall-Ports geöffnet. Über diese Ports

können die entsprechenden Telecontrol-Dienste ausgeführt werden, ohne dass deren Kommunikation durch die Firewall blockiert wird.

Tabelle 125: Ports für Telecontrol-Funktionalität

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

#### 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 126: 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 127: 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.<br>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 128: 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.<br>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 129: 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 129: WBM-Seite „Configuration of User Filter“ – Gruppe „User filter“

| Parameter | Bedeutung | |
|---|---|---|
| Add new user filter | Hier können Sie maximal 10 Filter anlegen.<br>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 130: 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 131: 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 132: 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 133: 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 und auch kryptografische Verfahren, die heute nicht mehr als sicher angesehen werden. |
| | Strong | Der Webserver erlaubt nur die TLS-Version 1.2 und starke Algorithmen. Ältere Software und ältere Betriebssysteme unterstützen eventuell TLS 1.2 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 134: 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 135: 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.<br>Geben Sie die Zykluszeit in Sekunden ein, mit der eine zyklische Aktualisierung durchgeführt wird.<br>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 136: 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.<br>In der Default-Einstellung ist die Authentifizierung ausgeschaltet. Zu Erhöhung des Security-Levels können Sie die Authentifizierung für das Scannen des Knotens erzwingen.<br>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 137: 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.<br>Geben Sie die Zykluszeit in Sekunden ein, mit der eine zyklische Aktualisierung durchgeführt wird.<br>Abhängig von Status wechselt die Beschriftung der Schaltfläche („Refresh“/„Start“/„Stop“). | |
| Source | Hier wählen Sie die Quelle der Diagnosemeldungen aus.<br>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 138: 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 139: 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.<br>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.<br>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.<br>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.<br>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 140: 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.<br>So ist es bspw. möglich, nur die Kommunikation von nur einem Port aufzuzeichnen oder von einer bestimmten IP-Adresse.<br>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 141: 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

# Tabellenverzeichnis

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