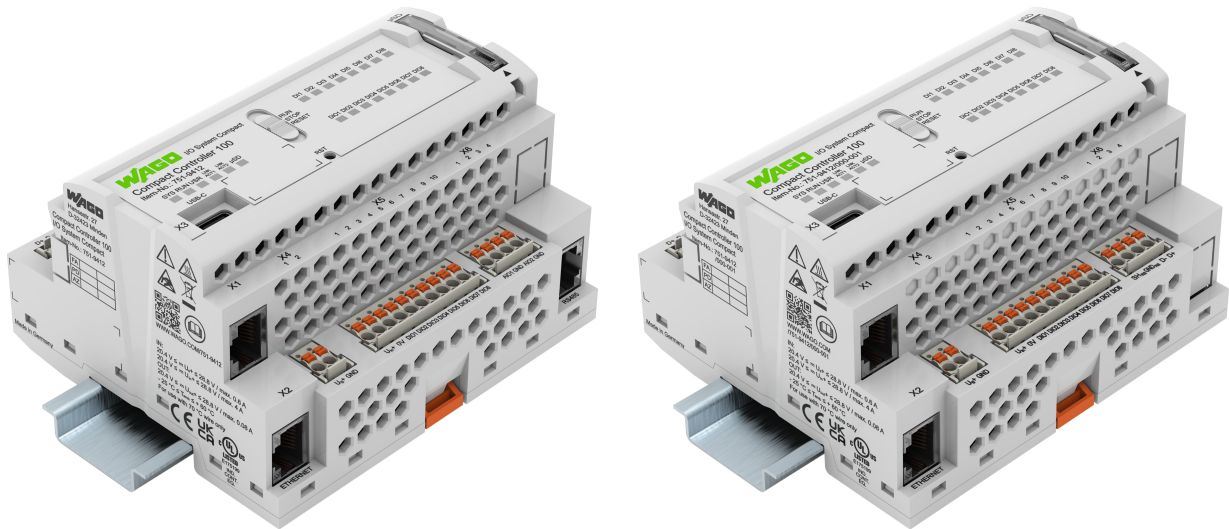


WAGO I/O System 751

SECURITY, Funktionsbeschreibungen YOCTO-Firmware

751-9412, 751-9412/000-001



© 2026 WAGO GmbH & Co. KG
Alle Rechte vorbehalten.

WAGO GmbH & Co. KG

Hansastraße 27
D - 32423 Minden

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

Technischer Support

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

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

E-Mail: ✉ documentation@wago.com

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

WAGO ist eine eingetragene Marke der WAGO Verwaltungsgesellschaft mbH.

Inhaltsverzeichnis

1 Bestimmungen.....	7
1.1 Gültigkeitsbereich	7
2 Cybersecurity.....	8
2.1 Bedrohungen.....	8
2.1.1 Bedrohung Cybersecurity allgemein.....	8
2.1.1.1 Angriffsziele aus Produktsicht.....	8
2.1.1.2 Angriffsvektor aus Produktsicht	8
2.1.2 Cybersecurityspezifische Bedrohungen.....	9
2.1.3 Schwachstellenanalyse	9
2.2 Angriffsflächen bei Netzwerkzugang	9
2.2.1 Angriffsflächen bei Netzwerkzugang – Überblick.....	9
2.2.2 SPS-Funktion	10
2.2.3 Nicht-gesicherter Feldbus	10
2.2.4 Nicht-gesicherter Lokalkbus	10
2.2.5 Root-Rechte	10
2.2.6 Programmierbarkeit	11
2.2.7 Engineering-/Service-Zugang	11
2.3 Angriffsflächen bei physikalischem Zugang.....	11
2.3.1 Angriffsflächen bei physikalischem Zugang – Überblick	11
2.3.2 Service-Schnittstelle.....	12
2.3.3 Betriebsartenschalter	12
2.3.4 Reset-Taster.....	12
2.3.5 Steckplatz für SIM-Karte.....	13
2.3.6 Steckplatz für Speicherkarte	13
2.4 Entstehende Angriffsflächen	13
2.4.1 Nicht-überwachte Indikatoren	13
2.5 Härtung und Cybersecurityfähigkeiten	13
2.5.1 Defense-in-depth-Prinzip	13
2.5.2 Referenzarchitektur	15
2.5.3 Härtungsmaßnahmen.....	15
2.5.3.1 Sichere Betriebsumgebung.....	15
2.5.3.2 Sichere Inbetriebnahme	16
2.5.3.3 Sicherer Betrieb	17
2.5.3.4 Sichere Außerbetriebnahme	18
2.5.4 Cybersecurityfähigkeiten	19
2.5.5 Cybersecurityservice	19
3 Überblick	21
4 Funktionen	22
4.1 Funktionsübersicht	22
4.2 Systemfunktionen.....	23
4.2.1 Normkonformität	23
4.2.2 Benutzerverwaltung	23
4.2.2.1 Allgemeine Einstellungen	24
4.2.2.1.1 Authentifizierungshinweis	24
4.2.2.1.2 Passwortgüte.....	24
4.2.2.1.3 Passwortänderungen	25
4.2.2.2 Systembenutzerkonten	25
4.2.2.2.1 Benutzerkonto „admin“	25
4.2.2.2.2 Benutzerkonto „root“.....	25
4.2.2.3 Lokale Benutzerverwaltung.....	26
4.2.2.3.1 Lokale Benutzerkonten.....	26
4.2.2.3.2 Lokale Benutzerrollen	27

4.2.2.4	Benutzerverwaltung über LDAP	28
4.2.2.5	Benutzeranmeldung	28
4.2.2.5.1	Loginfenster	28
4.2.2.5.2	Authentifizierungsdienst „OAuth2“	29
4.2.3	Ereignislogging	30
4.2.3.1	Interner Log-Speicher (Logging)	31
4.2.3.2	Externer Log-Server (Remote Logging)	31
4.2.4	Produkt- und Systemstatus	32
4.2.5	Echtzeituhr	33
4.2.5.1	Anzeige/Manuelle Einstellung	33
4.2.5.2	Automatische Einstellung	34
4.2.6	Laufzeitumgebung CODESYS V3	34
4.2.6.1	Speicherbereiche unter CODESYS V3	34
4.2.6.1.1	Programm- und Datenspeicher	34
4.2.6.1.2	Merkerbereich (Memory) und Retain-Bereich	34
4.2.6.2	CODESYS Web-Visualisierung	35
4.2.6.3	Security-Einstellungen in CODESYS	35
4.2.6.3.1	Sichere Kommunikation zwischen Entwicklungsumgebung und Steuerung	35
4.2.6.3.2	Integrität der übertragenen Projektdateien	35
4.2.7	Firmware-Update	35
4.2.7.1	Signaturen und Zertifikate für Updatebundle	36
4.2.8	Zertifikatsverwaltung	36
4.2.8.1	Truststore	37
4.2.8.2	Gerätezertifikate	38
4.2.9	Webserver	39
4.2.9.1	CORS-Policy	40
4.2.10	Open-Source-Lizenzen	41
4.2.11	WAGO Device-Access	41
4.2.11.1	Geräte-Scan	41
4.2.12	Factory-Reset	42
4.3	Hardwarefunktionen	42
4.3.1	Betriebsartenschalter/Reset-Taster	42
4.3.1.1	Betriebsartenschalter	42
4.3.1.2	Reset-Taster	43
4.3.2	Kommunikationsschnittstelle	43
4.3.3	USB-C-Service-Schnittstelle	43
4.3.4	OnBoard-I/O	44
4.3.4.1	Analogeingänge AI1, AI2	44
4.3.4.1.1	AI 0 ... 10 V	44
4.3.4.1.2	AI -10 ... 10 V	44
4.3.4.1.3	AI 0 ... 20 mA	45
4.3.4.1.4	AI 4 ... 20 mA	45
4.3.4.1.5	AI 3,6 ... 21 mA	45
4.3.4.2	Analogein-/ausgänge AIO1, AIO2	45
4.3.4.2.1	AI 0 ... 10 V, -10 ... +10 V, 0 ... 20 mA, 4 ... 20 mA, 3,6 ... 21 mA	46
4.3.4.2.2	AO 0 ... 10 V	46
4.3.4.2.3	AO -10 ... +10 V	46
4.3.4.2.4	AO -12 ... +12 V	46
4.3.4.2.5	AO 0 ... 20 mA	46
4.3.4.2.6	AO 0 ... 22 mA	47
4.3.4.2.7	AO 4 ... 20 mA	47
4.3.4.3	Temperatureingänge PT1+/PT1-, PT2+/PT2-	47
4.3.4.3.1	Pt100, Pt200, Pt500, Pt1000	48
4.3.4.3.2	Ni100, Ni1000 (TK6180), Ni1000 (TK5000)	48
4.3.4.3.3	Ni120	48
4.3.4.3.4	Potentiometer 0 ... 1,2 kOhm	48
4.3.4.3.5	Potentiometer 0 ... 5 kOhm	49
4.3.4.4	Digitaleingänge DI	49

4.3.4.5	Digitalein-/ausgänge DIO	49
4.3.4.5.1	DI 0/24 V	50
4.3.4.5.2	DO 0/24V	50
4.4	Konfigurationsfunktionen	50
4.4.1	Web-based Management (WBM)	50
4.4.1.1	Allgemeine Bedienelemente	51
4.4.1.2	Menüband (Geräteaktionen)	51
4.4.1.3	Gerät	51
4.4.1.4	Arbeitsbereich	52
4.4.1.4.1	I/O-Check	52
4.4.1.4.2	Einstellungen	56
4.4.1.4.3	Neustart	61
4.4.1.4.4	Firmware	61
4.4.1.4.5	Backup/Restore	62
4.4.1.4.6	Geräte-Log	63
4.4.1.5	Meldungsfenster	64
4.5	Netzwerkfunktionen	66
4.5.1	Netzwerkconfiguration	66
4.5.1.1	Konfiguration für SECURITY-Anforderungen	66
4.5.1.2	Schnittstellenkonfiguration	67
4.5.1.2.1	Bridge-und Portkonfiguration	67
4.5.1.3	Hostname/Domainadressen	69
4.5.1.3.1	Hostname	69
4.5.1.3.2	Domainadressen	69
4.5.2	Netzwerksicherheit	70
4.5.2.1	Bereitstellen einer sicheren Netzwerkkumgebung	70
4.5.2.2	Firewall	70
4.5.2.2.1	MAC-Adressenfilter	70
4.5.2.2.2	ServiceRules	71
4.5.2.2.3	IP-Adressenfilter	71
4.5.2.2.4	IP-Forwarding-Filter	72
4.5.2.2.5	Flood/Broadcast Protection	73
4.5.2.3	IPsec	73
4.5.3	Netzwerkdienste	75
4.5.3.1	DHCP-Client	75
4.5.3.2	SSH-Dienst	75
4.6	Speicherfunktionen	76
4.6.1	Automount	76
4.6.2	Datensicherung	76
4.6.2.1	Backup-Funktion	76
4.6.2.2	Restore-Funktion	76
4.7	Diagnosefunktionen	77
4.7.1	Diagnose über Anzeigeelemente	77
4.7.2	Diagnose über WBM oder WAGO Device Manager	77
4.7.2.1	Abbildung der LEDs	77
4.7.2.2	Verdrahtungstest (I/O-Check)	77
4.7.2.3	Ereignisprotokoll (Geräte-Log)	77
5	In Betrieb nehmen	79
5.1	Einschalten des Controllers	79
5.2	Einstellen einer IP-Adresse	79
5.2.1	Einstellen einer IP-Adresse über das WBM	80
5.2.2	Zuweisen einer IP-Adresse mit DHCP	80
5.3	Passwörter ändern	80
5.4	Benutzer verwalten	81
5.4.1	Lokale Benutzerrollen und -konten verwalten	81
5.4.1.1	Lokale Benutzerkonten verwalten	81

5.4.1.2	Lokale Benutzerrollen verwalten	82
5.5	Ausschalten/Neustart.....	83
6	Konfigurieren.....	84
6.1	Konfigurieren im WBM.....	84
7	Service	86
7.1	Firmwareänderungen	86
7.1.1	Firmware-Update mit WBM durchführen	86
7.2	Reset-Funktionen auslösen	88
7.2.1	Warmstart-Reset	88
7.2.2	Kaltstart-Reset.....	88
7.2.3	Software-Reset (Neustart).....	89
7.2.4	Factory-Reset.....	89
7.3	CODESYS Applikationen starten/stoppen	90
7.3.1	CODESYS Applikationen starten	90
7.3.2	CODESYS Applikationen stoppen	90
7.4	Daten sichern und wiederherstellen	90
7.4.1	Backup durchführen	91
7.4.2	Restore durchführen	91
7.5	WDX-Methoden für Fertigung	92
7.6	Zertifikate erstellen und verwalten.....	92
7.6.1	Gerätezertifikate erstellen	92
7.6.1.1	Selbstsignierte Zertifikate	92
7.6.1.2	Über eine externe PKI signierte Zertifikate	93
7.6.2	Extern erstellte und signierte Gerätezertifikate laden.....	94
8	Diagnose.....	96
8.1	Diagnose über Anzeigeelemente	96
8.2	Diagnose über WBM	96
8.2.1	Verdrahtungstest durchführen.....	96
8.2.2	Geräte-Log einsehen.....	97
8.3	Systemintegrität prüfen	98

1 Bestimmungen

1.1 Gültigkeitsbereich

Das vorliegende Dokument gilt für folgende Produkte:

751-9412 (Compact Controller 100) (Compact Controller 100; 8DI 8DIO 2AI 2AIO 2RTD 2RS 2ETH; SD)

Version Firmware	01.02.03(03)
Produktdetailseite	www.wago.com/751-9412

751-9412/000-001 (Compact Controller 100) (Compact Controller 100; 8DI 8DIO 2AI 2RTD 2RS 2ETH; SD)

Version Firmware	01.02.03(03)
Produktdetailseite	www.wago.com/751-9412/000-001

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

Mitgeltes Dokument

☞ **Produkthandbuch** des verwendeten Produktes

Information

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

2 Cybersecurity

2.1 Bedrohungen

2.1.1 Bedrohung Cybersecurity allgemein

Eintrittswahrscheinlichkeit und Schwere von Ereignissen

Produkte für die industrielle Automatisierung können in sehr unterschiedlichen Anlagen und Anwendungen eingesetzt werden. Je nach Anwendung können die Anforderungen an die **Schutzziele** der Cybersecurity (Integrität, Verfügbarkeit oder Vertraulichkeit von Daten) unterschiedlich hoch sein. Ebenso unterschiedlich sind entsprechend auch die Anreize für potenzielle Angreifer und die Schwere eintretender Ereignisse der Cybersecurity.

Als Hersteller können wir beschreiben, unter welchen Umständen auf welche Datenbereiche, Schnittstellen oder Funktionen unseres Produktes unautorisiert zugegriffen werden kann. Angriffsziele können aus **Produktsicht** betrachtet werden. Als Hersteller können wir Anweisungen geben, wie mit den Cybersecurityfähigkeiten des Produktes die Wahrscheinlichkeit eines unautorisierten Zugriffs reduziert werden kann.

Der Betreiber muss aus **Anwendungssicht** prüfen, welcher Schaden entstehen kann, welches Sicherheitsniveau erforderlich ist und ob zusätzliche Maßnahmen zur Erhöhung der Sicherheit erforderlich sind. Ein Kriterium für die Angemessenheit des Sicherheitsniveaus ist beispielsweise, ob im konkreten Anwendungsfall personenbezogene Daten verarbeitet werden oder nicht. Die tatsächlichen Auswirkungen unautorisierter Zugriffe im jeweiligen konkreten Anwendungsfall kann nur der Betreiber beurteilen.

2.1.1.1 Angriffsziele aus Produktsicht

Aus Produktsicht können mindestens die folgenden physikalischen oder logischen Objekte ein Angriffsziel darstellen:

- Produktfunktion stören (Verfügbarkeit einschränken).
- Daten manipulieren (auf Auswertungen, Entscheidungen oder Systemverhalten Einfluss nehmen).
- Daten unautorisierten Personen (Dritte) zugänglich machen.
- Zugriff auf verbundene andere Systeme erhalten.

2.1.1.2 Angriffsvektor aus Produktsicht

Aus Produktsicht können mindestens die folgenden grundlegenden Mechanismen einen Angriffsvektor darstellen:

- Unterbrechung der Spannungsversorgung:
Einschränkung der Verfügbarkeit (DoS) oder Vorbereitung weiterer Attacken
- Zugriff auf ungeschützte Schnittstellen:
Unautorisierte Betätigung der Schnittstellen; vielfältige Angriffsziele, potenziell auch die Übertragung manipulierter Soft-/Firmware
- Zugriff auf unverschlüsselte Daten:
Unautorisierte Verwendung, Weitergabe oder Manipulation von Daten
- Veränderung des Aufbaus, der Konfiguration oder der Programmierung des Produktes:
Vielfältige Angriffsziele, potenziell auch die Kompromittierung weiterer verbundener Systeme

2.1.2 Cybersecurityspezifische Bedrohungen

Konkrete Bedrohungen können nur bei Kenntnis der jeweiligen Anlage und Anwendung beurteilt werden. Das Beurteilen von Bedrohungen, die sich aus der Bedeutung übertragener Daten ergeben, muss der Betreiber selbst durchführen. Unabhängig von der Beurteilung übertragener Daten können grundlegende Arten von Bedrohungen für den spezifischen Produkttyp benannt werden.

Grundlegende Bedrohungsarten spezifisch für den Produkttyp: Controller CC100 V2 Secure

- Stören der Kommunikation im Netzwerk:
Indem die Netzwerkadresse des Produktes manipuliert wird, können Adresskonflikte herbeigeführt, die Kommunikation unterbrochen oder Daten fehlgeleitet werden.
- Aneignen von Informationen über Prozesse der Anlage:
Durch Mitschneiden der Prozesseingangs- oder Prozessausgangsdaten können Informationen zu in der Anlage ablaufenden Prozessen gewonnen werden. Diese Kenntnisse ermöglichen, weitere Schwachstellen für Angriffe der Cybersecurity zu identifizieren.
- Stören von Abläufen oder Verursachen von Schäden in der Anlage:
Durch Manipulation von Prozesseingangsdaten kann die überlagerte Steuerung zum Erzeugen falscher Vorgabewerte für dezentrale Automatisierungsgeräte veranlasst werden. Durch Manipulation von Prozessausgangsdaten können Aktoren der Feldebene zum Ausführen falscher Vorgänge veranlasst werden.

2.1.3 Schwachstellenanalyse

Produkte haben aufgrund ihrer Produktfunktionen technische Grenzen. Diese technischen Grenzen können in der Cybersecurity eine Schwachstelle darstellen.

Wenn der Betreiber diese Schwachstellen durch eigene technische oder organisatorische Maßnahmen kompensiert, kann das Produkt dennoch sicher verwendet werden.

Angriffsflächen sind Produkteigenschaften, welche eine bekannte Cybersecurity-Schwachstelle darstellen, falls der Betreiber keine geeigneten Schutzmaßnahmen ergreift.

Hinweis: Der Betreiber ist dafür verantwortlich, alle dokumentierten Angriffsflächen hinsichtlich der Eintrittswahrscheinlichkeit und Schwere von Vorfällen zu bewerten und angemessene Maßnahmen zu ergreifen. Die Schwachstellenanalyse muss auf potentielle Schwachstellen ausgedehnt werden, welche sich aus der Integration in die jeweilige Anlage und Anwendung ergeben.

Die Schwachstellenanalyse unterstützt das Erreichen der Schutzziele Integrität, Verfügbarkeit oder Vertraulichkeit von Daten.

2.2 Angriffsflächen bei Netzwerkzugang

2.2.1 Angriffsflächen bei Netzwerkzugang – Überblick

Das Produkt ist für den Einsatz in einem geschützten Netzwerksegment bestimmt.

Folgende Angriffe sind in einem ungeschützten Netzwerksegment durch unautorisierten Zugriff möglich:

Daten können ausgelesen werden. Daten können manipuliert werden. Daten können an unautorisierte Personen (Dritte) weitergegeben werden.

Folgende Daten können beispielsweise betroffen sein:

- Produkt-/Gerätedaten, Prozessdaten, Konfigurationsdaten, Registerdaten, Lokalbusdaten

Konfigurationen können ausgelesen werden. Konfigurationen können manipuliert werden. Konfigurationen können an unautorisierte Personen (Dritte) weitergegeben werden.

Folgende Konfigurationen können betroffen sein:

- Produkt-/Gerätekonfigurationen, Projektkonfigurationen, Netzwerkkonfigurationen

Soft-/Firmware kann ausgelesen werden. Soft-/Firmware kann manipuliert werden. Soft-/Firmware kann an unautorisierte Personen (Dritte) weitergegeben werden.

Folgende Soft-/Firmware kann betroffen sein:

- Soft-/Firmware des Produktes, Software von Service-/Hilfsmitteln

Systeme können ausgelesen werden. Systeme können manipuliert werden. Systeme können kompromittiert werden.

Folgende Systeme können betroffen sein:

- I/O-System, weitere verbundene Systeme

2.2.2 SPS-Funktion

Die Funktion der speicherprogrammierbaren Steuerung (SPS) ermöglicht in Netzwerken Prozessdaten von Sensoren aufzunehmen und Aktoren anzusteuern.

Die Cybersecurityfähigkeit der Funktion der speicherprogrammierbaren Steuerung (SPS) ist abhängig von vielen Faktoren.

Wenn die Funktion der speicherprogrammierbaren Steuerung (SPS) nicht ausreichend gesichert ist, kann über unautorisierte Benutzer und/oder Schadsoftware das Produkt ausgelesen oder manipuliert werden.

2.2.3 Nicht-gesicherter Feldbus

Der Feldbus verbindet leitungsgebunden den Feldbuskoppler mit den Sensoren und Aktoren des Bussystems und dient dem Datenaustausch zwischen den Komponenten.

Ein nicht-gesicherter Feldbus hat keine Cybersecurityfähigkeiten wie Authentifizierung, Integritätsschutz und Verschlüsselung.

Nicht-gesicherte Feldbusse sind beispielsweise: Modbus TCP, BACnet.

2.2.4 Nicht-gesicherter Lokalbus

Der Lokalbus ist ein interner Bus, der die Datenverbindung zwischen den Kopfstationen (Feldbuskoppler oder Controller) und den I/O-Modulen herstellt. Die Übertragung der Daten erfolgt unverschlüsselt.

Der Lokalbus stellt eine direkte Verbindung zwischen den Komponenten eines I/O-Systems her. Der Lokalbus kann mit einem Verbindungskabel (RJ-45) verlängert werden.

Der Lokalbus hat keine Cybersecurityfähigkeiten wie Authentifizierung, Integritätsschutz und Verschlüsselung.

2.2.5 Root-Rechte

Das Benutzerkonto „root“ enthält uneingeschränkte Rechte.

Ein aktiviertes Benutzerkonto „root“ ermöglicht Modifikationen an der Firmware eines Produktes. Das aktivierte Benutzerkonto „root“ hat Zugriff und die Berechtigung für die Modifikation aller Funktionen, Konfigurationen und Zertifikate eines Produktes.

Ein aktiviertes Benutzerkonto „root“ ist für den Zugriff auf das Betriebssystem Linux des Produktes notwendig.

Wenn der Zugriff auf das aktivierte Benutzerkonto „root“ nicht ausreichend gesichert ist, kann über unautorisierte Benutzer und/oder Schadsoftware das Produkt ausgelesen oder manipuliert werden.

2.2.6 Programmierbarkeit

Die Programmierbarkeit eines Produktes ermöglicht dem Benutzer Applikation selbst zu programmieren und ausführen. Dies kann in einer Laufzeitumgebung oder über ein Betriebssystem erfolgen.

Die Werkseinstellung des Produktes ermöglicht die volle Auslastung der Systemressourcen mit selbstprogrammierten Applikationen.

Die Verfügbarkeit der Systemfunktionen einer selbstprogrammierten Applikationen ist abhängig von vielen Faktoren.

- Die Laufzeitumgebung hat ein Ressourcenmanagement.

Ein nicht-genutztes Ressourcenmanagement der Laufzeitumgebung kann zu einem Ausfall des Normalbetriebes führen.

Eine Laufzeitumgebung ist beispielsweise: CODESYS.

2.2.7 Engineering-/Service-Zugang

Über den Engineering-/Service-Zugang werden Konfigurationen und Parametrierungen vorgenommen.

Für den Engineering-/Service-Zugang ist die Ausführung eines Engineering-, Konfigurations- und Parametriertools auf ein externes Engineeringgerät (z. B. PC oder Laptop) erforderlich.

Die Cybersecurityfähigkeit eines Engineeringgerätes ist abhängig von vielen Faktoren.

Insbesondere von:

- Dem Betriebssystem
- Den Benutzerrechten
- Der Anbindung in wechselnde Netzwerke (z. B. öffentlich zugängliche)
- Dem Anschluss mobiler Datenträger

Wenn das Engineeringgerät nicht ausreichend gesichert ist, kann über unautorisierte Benutzer und/oder Schadsoftware das Produkt ausgelesen oder manipuliert werden.

2.3 Angriffsflächen bei physikalischem Zugang

2.3.1 Angriffsflächen bei physikalischem Zugang – Überblick

Das Produkt ist für den Einsatz in einem physikalisch geschützten Zugangsbereich bestimmt.

Folgende Angriffe sind in einem physikalisch ungeschützten Zugangsbereich durch unautorisierten Zugriff möglich:

Verbindungen und damit die Erreichbarkeit des Produktes können unterbrochen oder ausgesetzt werden.

Folgende Verbindungen können betroffen sein:

- Netzwerkverbindung, Lokalbus, Service-Schnittstellen

Daten können ausgelesen werden. Daten können manipuliert werden. Daten können an unautorisierte Personen (Dritte) weitergegeben werden.

Folgende Daten können beispielsweise betroffen sein:

- Produkt-/Gerätedaten, Prozessdaten, Konfigurationsdaten, Registerdaten, Lokalbusdaten

Das Produkt kann auf Werkseinstellung zurückgesetzt werden. Dadurch ist ein Zugriff auf das Produkt möglich. Folgende Einstellungen können betroffen sein:

- Produkt-/Geräteeinstellungen

Komponenten des modularen I/O-Systems können ausgetauscht werden. Komponenten, die manipuliert wurden, können in das System eingesetzt werden.

Folgende Komponenten können betroffen sein:

- Komponenten des I/O-Systems

Die Soft-/Firmware kann ausgetauscht werden. Soft-/Firmware, die manipuliert wurde, kann in das System übertragen werden.

Folgende Soft-/Firmware kann betroffen sein:

- Soft-/Firmware der Komponenten des I/O-Systems

2.3.2 Service-Schnittstelle

Die Service-Schnittstelle dient als Konfigurations-, Programmier- und Firmwareschnittstelle.

Die Konfiguration und die Programmierung können ausgelesen und geändert werden. Netzwerkeinstellungen können vorgenommen werden.

2.3.3 Betriebsartenschalter

Mit dem Betriebsartenschalter wird die Betriebsart (STOP, RUN und RESET) eingestellt. Mit STOP wird die geladene Applikation gestoppt. Mit RESET wird die Applikation zurückgesetzt.

In Kombination mit dem Reset-Taster werden Geräteeinstellungen und Zugangsdaten auf Werkseinstellungen zurückgesetzt.

Alle Applikationen und Parameter werden gelöscht.

2.3.4 Reset-Taster

Mit dem Reset-Taster kann ein Neustart der Firmware durchgeführt werden.

Einstellungen und die Zugangsdaten können auf Werkseinstellungen zurückgesetzt werden.

In Kombination mit dem Betriebsartenschalter werden Geräteeinstellungen und Zugangsdaten auf Werkseinstellungen zurückgesetzt.

Alle Applikationen und Parameter werden gelöscht.

2.3.5 Steckplatz für SIM-Karte

Der Steckplatz für SIM-Karte dient zur Platzierung einer SIM-Karte. Die SIM-Karte dient der GPRS-Verbindung des Produktes. Die GPRS-Verbindung ermöglicht die Fernwartung des Produktes.

Diese Funktion wird derzeit nicht unterstützt.

2.3.6 Steckplatz für Speicherkarte

Der Steckplatz für Speicherkarte enthält eine Speicherkarte mit spezifischen Daten. Mit einer Speicherkarte können Daten, Bootprojekte oder eine Soft-/Firmware in das Produkt oder in das System übertragen werden.

Diese Funktion wird derzeit nicht unterstützt.

2.4 Entstehende Angriffsflächen

2.4.1 Nicht-überwachte Indikatoren

Das Produkt ist für den Einsatz in einer sicheren Betriebsumgebung bestimmt.

Das Produkt verfügt nicht über die Möglichkeiten, Indikatoren für die Vorbereitung oder Durchführung eines Cybersecurityangriffes zu erkennen.

Das Produkt kann bei Auftreten entsprechender Ereignisse oder Vorgänge keine ausreichenden eigenen Gegenmaßnahmen ergreifen. Fehlende Eigendiagnose gibt Angreifern die Möglichkeit, Schwachstellen durch Experimentieren zu finden und auszunutzen.

Beispiele für Indikatoren für die Vorbereitung oder Durchführung eines Cybersecurityangriffes sind:

- Veränderte – meist erhöhte – Netzwerkaktivität
- Veränderte – meist erhöhte – Auslastung der Hardware
- Häufige aufeinander folgende Änderungen der Konfigurationen

2.5 Härtung und Cybersecurityfähigkeiten

2.5.1 Defense-in-depth-Prinzip

Das Produkt ist ein Gerät mit offenen Schnittstellen und Ports und ist für den Einsatz in einem geschützten Netzwerksegment bestimmt.

Für den Einsatz müssen Schutzmaßnahmen entsprechend des Einsatzbereiches vorgenommen werden.

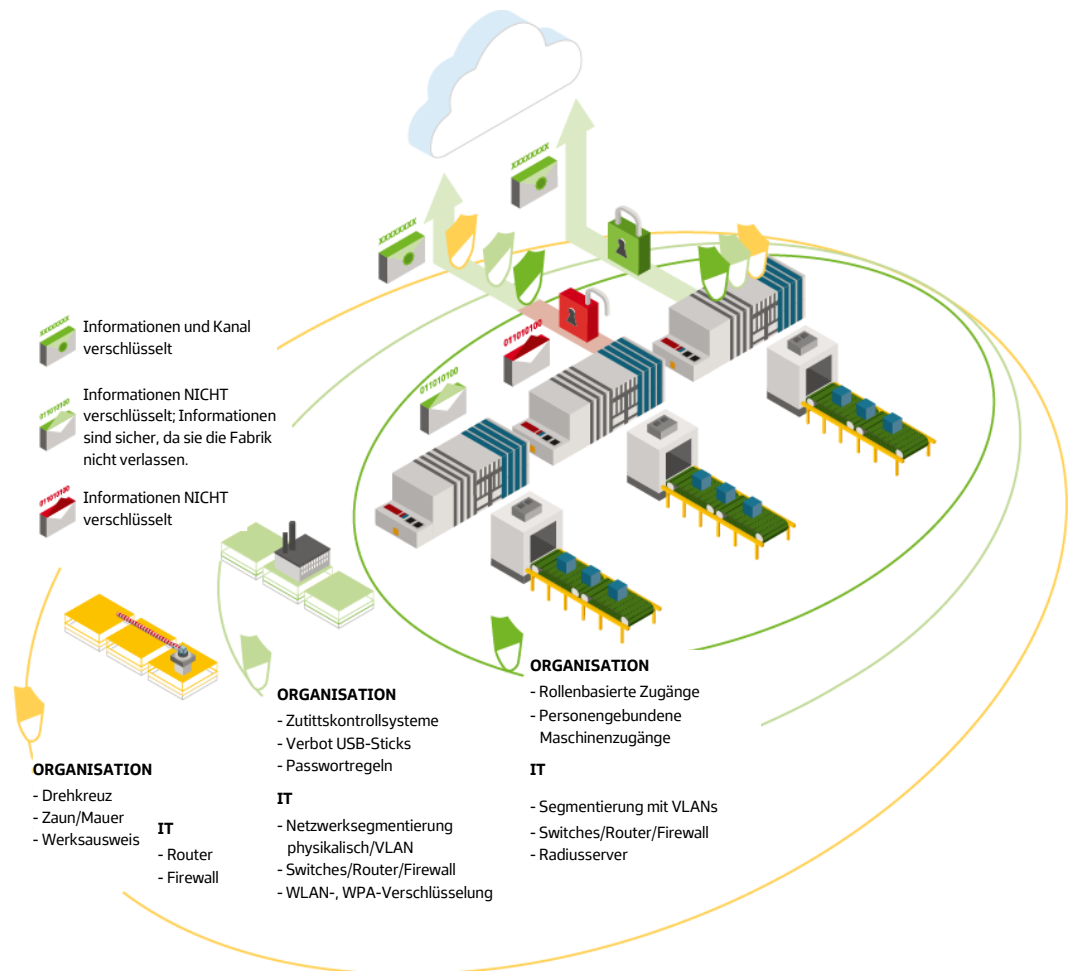


Abbildung 1: Zwiebelschalenmodell (Beispiel)

Der Betreiber einer Anlage muss organisatorische und technische Sicherheitsmaßnahmen miteinander kombinieren, um Bedrohungen der Cybersecurity erfolgreich abzuwehren.

Keine einzelne Sicherheitsmaßnahme bietet umfassenden Schutz. Beispielsweise spielt die Härte einer Tresortür (technische Sicherheitsmaßnahme) keine Rolle, während die Tür zum Einlagern oder Auslagern gerade offen steht (organisatorische Sicherheitsmaßnahme).

Die Funktion mancher Produkte erfordert es, dass innerhalb der Vertrauensgrenzen („Trust Boundaries“) oder innerhalb bestimmter Zeiträume Vorgänge ohne Schutzfunktionen („Tresortür offen“) erfolgen. Im Produkt fehlende Schutzfunktionen müssen dann durch die vom Betreiber verantwortete Einsatzumgebung realisiert werden.

Die getroffenen organisatorischen und technischen Sicherheitsmaßnahmen müssen wie die Schalen einer Zwiebel alle verwundbaren Zugänge oder Übertragungswege umhüllen und Angriffsflächen abdecken. Die getroffenen Sicherheitsmaßnahmen müssen zudem so gestaltet sein, dass bei Überwinden einer Maßnahme die anderen Maßnahmen weiterhin schützend wirken.

Als Hilfestellung für die Auslegung der Sicherheitsarchitektur enthält diese Dokumentation Angaben zu aus Produktsicht erkennbaren, erforderlichen Maßnahmen: **Härtungsmaßnahmen** [► 15].

2.5.2 Referenzarchitektur

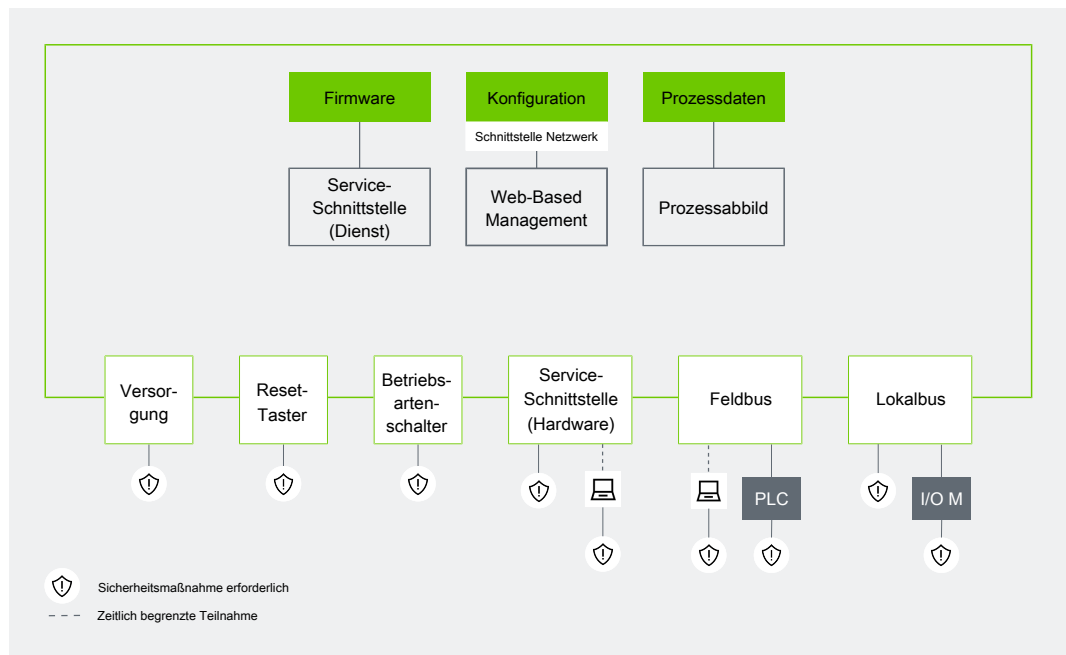


Abbildung 2: Referenzarchitektur

2.5.3 Härtingsmaßnahmen

Die beschriebenen Härtingsmaßnahmen stellen keine Alternativen zueinander dar. Damit ein guter Schutz gegeben ist, müssen die unterschiedlichen Härtingsmaßnahmen ergänzend zueinander umgesetzt werden.

2.5.3.1 Sichere Betriebsumgebung

Das Produkt darf nur in einer sicheren Betriebsumgebung betrieben werden.

Eine sichere Betriebsumgebung trägt dazu bei, verschiedene Angriffe zu vermeiden. Eine sichere Betriebsumgebung erfüllt mindestens die folgenden Anforderungen:

- Physikalisch geschützter Zugang
- Geschütztes Netzwerksegment
- Protokollierte Zugänge und Zugriffe
- Überwachung auf verdächtige Ereignisse oder Vorgänge

Physikalisch geschützter Zugang

Das Produkt ist ein Gerät mit zugänglichen Bedienelementen, Anschlüssen und Speichermöglichkeiten.

Es darf nur in geeigneten Gehäusen, Schränken oder elektrischen Betriebsräumen eingebaut werden, die mindestens die folgenden Anforderungen erfüllen:

- Zugangsbereich ist geschützt.
- Zugang erfolgt nur autorisiert.
- Die Verlängerung des Lokalbuses führt nicht nach außen.
- Nur notwendige Anschlüsse führen physikalisch nach außen.

Geschütztes Netzwerksegment

Das Produkt ist ein Gerät mit offenen Schnittstellen und Netzwerkports.

Es darf nur in einem geschützten Netzwerksegment eingesetzt werden, das mindestens die folgenden Anforderungen erfüllt:

- Es besteht keine ungeschützte Verbindung zum Internet.
- Es besteht keine ungeschützte Verbindung zu weiteren Netzwerksegmenten.
- Zugriffe erfolgen autorisiert gemäß der Referenzarchitektur.
- Alle Netzwerkteilnehmer befinden sich in einem geschützten Netzwerksegment.

Protokollierte Zugänge und Zugriffe

Das Produkt bedarf in bestimmten Situationen einer zeitlich begrenzten Herabsetzung der Sicherheit. Eine zeitlich begrenzte Herabsetzung der Sicherheit kann beispielsweise bei Engineering-/Servicetätigkeiten oder in einem Fehlerfall notwendig sein.

Eine Protokollierung muss mindestens die folgenden Ereignisse erfassen:

- Verbindung eines Engineeringgerätes
- Zugriff auf das geschützte Netzwerksegment (z. B. Änderung der Grenze des geschützten Netzwerksegmentes, Deaktivieren der Firewall des Netzwerkes)
- Zugang in den physikalisch geschützten Bereich (z. B. Service-Personal)

Überwachung auf verdächtige Ereignisse oder Vorgänge

Eine Überwachung muss mindestens die folgenden Ereignisse und Vorgänge erfassen:

- Veränderte, insbesondere verdächtig erhöhte Netzwerkaktivität

2.5.3.2 Sichere Inbetriebnahme

Eine sichere Inbetriebnahme des Produktes trägt dazu bei, verschiedene Angriffe zu vermeiden. Eine sichere Inbetriebnahme erfüllt mindestens die folgenden Anforderungen:

- Geänderte Zugangsdaten
- Geschützte Netzwerkzugänge
- Geeignete Aufteilung des Anwendungsprogramms in priorisierte Tasks

Zugangsdaten

- Ändern Sie alle frei zugänglich und dokumentierten Zugangsdaten.

Die Zugangsdaten sind im  **Produkthandbuch** frei zugänglich und dokumentiert.

Die folgenden Einstellungen müssen mindestens erfüllt sein:

- Passwort für Benutzerkonto "admin" wurde vergeben.
- Unbenutzte Netzwerkports sind deaktiviert.
- Die Netzwerkports benutzter Dienste sind geändert, sofern dies am Produkt selbst und auch der Gegenseite sinnvoll umsetzbar ist.
- Unbenutzte Schnittstellen sind deaktiviert.
- Unbenutzte Funktechnologie ist deaktiviert.

Netzwerkzugänge

- Schützen Sie die Netzwerkzugänge.

Die folgenden Anforderungen müssen mindestens erfüllt sein:

- Funktionen für Netzwerkschutz des Produktes werden verwendet.
Wenn verfügbar: z. B. MAC-Filter
- Gesichertes Protokoll wird verwendet.
Wenn verfügbar: z. B. HTTPS, SFTP
- Nur notwendige Schnittstellen sind aktiviert.

- Nur notwendige Netzwerkports sind aktiviert.
- Nur notwendige Dienste sind aktiviert.

Aufteilung des Anwendungsprogramms

- Teilen Sie Ihr Anwendungsprogramm auf.

Die folgenden Anforderungen müssen mindestens erfüllt sein:

- Priorisierung der Teile des Anwendungsprogramms
- Zuordnung der Teile des Anwendungsprogramms zu Taskprioritäten (Entwicklungsumgebung)

2.5.3.3 Sicherer Betrieb

Ein sicherer Betrieb des Produktes trägt dazu bei, verschiedene Angriffe zu vermeiden. Ein sicherer Betrieb erfüllt mindestens die folgenden Anforderungen:

- Zeitlich begrenzte physikalische Zugänge bei Engineering-/Servicetätigkeiten oder Fehlerfall
- Zeitlich begrenzte Zugriffe und Zugänge bei Engineering-/Servicetätigkeiten oder Fehlerfall
- Logging von Securityereignissen/-vorgängen
- Handlung nach einem Securityereignis/-vorgang
- System Integritätsprüfungen nach Änderungen
- Verwendung geprüfter und aktueller Firmware/-Updates
- Verwendung von Hilfsmitteln zur Überprüfung der Cybersecurity

Zugriffe und Zugänge bei Engineering-/Servicetätigkeiten oder Fehlerfall

Engineering- oder Servicetätigkeiten erfordern oft Zugang auf Daten oder Konfiguration des Produkts. Daher muss der Betreiber sicherstellen, dass die verwendeten Drittgeräte sowie die zum Produkt hergestellte Verbindung sicher sind.

- Gewähren Sie Zugriffe und Zugänge nur zeitlich begrenzt.

Mindestens die folgenden Zugriffe/Zugänge müssen zeitlich begrenzt werden:

- Zugriff auf Kommunikationssoftware
- Zugriff auf Schnittstellen
- Zugriff mit erhöhten Rechten

Logging Securityereignisse

- Loggen Sie Securityereignisse.

Die folgenden Anforderungen an das Logging von Securityereignissen müssen mindestens erfüllt sein:

- Logging-Funktion des Produktes ist eingerichtet.
- Logging-Maßnahmen für Securityereignisse, die das Produkt nicht loggt, sind eingerichtet.
- Logging-Maßnahmen für das Netzwerk sind eingerichtet.

WAGO empfiehlt die Verwendung von „System Logging Protocol“ (Syslog).

Nach einem Securityereignis

- Handeln Sie nach einem Securityereignis.

Die folgenden Handlungen nach einem Securityereignis müssen mindestens erfüllt werden:

- Ist- und Sollkonfigurationsdaten vergleichen.

Systemintegritätsprüfungen

- Prüfen Sie nach Änderungen die Integrität Ihres Systems.

Die folgenden Prüfungen müssen nach Änderungen der Konfigurationen mindestens durchgeführt werden:

- Prüfung der Prüfsumme der Konfigurationen
- Prüfung der Firewall

Geprüfte und aktuelle Firmware(-Updates)

- Verwenden Sie nur geprüfte und aktuelle Firmware(-Updates).

Die folgenden Anforderungen sind Merkmale einer geprüften und aktuellen Firmware/-Updates:

- Prüfsumme wurde erfolgreich verifiziert (Integritätsprüfung).

WAGO empfiehlt die Verwendung von aktueller Firmware.

Die aktuelle Version einer Firmware entspricht dem aktuellen Stand der Technik und der Sicherheit. Vorherige Versionen einer Firmware können Schwachstellen in Technik und Sicherheit aufweisen.

Geprüfte und aktuelle WAGO Firmware(-Updates) und Informationen zur Installation erhalten Sie unter:

🔗 <https://downloadcenter.wago.com>

Weitere Informationen erhalten Sie beim:

🔗 [Technischen Support](#)

Hilfsmittel

- Nutzen Sie weitere Hilfsmittel zur Überprüfung der Security.

Die folgenden Hilfsmittel können zur Überprüfung der Cybersecurity Ihres Systems helfen:

- System Logging Protocol (Syslog)
- Management von Zertifikaten
- WAGO IO-Update 750 (auf Anfrage über den technischen Support)

2.5.3.4 Sichere Außerbetriebnahme

Eine sichere Außerbetriebnahme des Produktes trägt dazu bei, verschiedene Angriffe zu vermeiden. Eine sichere Außerbetriebnahme erfüllt mindestens die folgenden Anforderungen:

- Gelöschte Daten im Produkt
- Gelöschte Daten des Produktes in der Umgebung

Daten im Produkt

- Löschen Sie alle im Produkt gespeicherten Daten.

Die folgenden Anforderungen müssen mindestens erfüllt sein:

- Produkt ist auf Werkseinstellungen zurückgesetzt.
- Daten, die nicht gelöscht werden können, sind überschrieben (z. B. mit „0“).
- Bei Verdacht auf nicht gelöschte, sensible Daten: Verschrottung durch einen für Cybersecurity qualifizierten Entsorgungsdienstleister veranlassen.

Daten des Produktes in der Umgebung

- Löschen Sie alle vom Produkt gespeicherten Daten in der Umgebung.

Die folgenden Anforderungen müssen mindestens erfüllt sein:

- Konfigurationen des Produktes in der Projektierumgebung sind gelöscht.

2.5.4 Cybersecurityfähigkeiten

Produktgehäuseschutz

Ein physikalischer Schutz des Produktgehäuses zeigt ein unautorisiertes Öffnen des Produktgehäuses an.

- Das Produktgehäuse ist ab Werk mit einem Security Siegel versiegelt.

Sitzungssperrung

Eine Sitzungssperrung schützt bei Inaktivität vor unautorisiertem Zugriff. Eine Sitzungssperrung kann bei Inaktivität nach einem konfigurierbaren Zeitraum oder durch aktives Abmelden erfolgen. Durch Authentifizierung des Benutzers wird der Zugriff wieder hergestellt.

- Die Sitzungssperre erfolgt über das Betriebssystem des Engineeringgerätes.
- Die Sitzungssperre des Engineeringgerätes ist eingerichtet.

Secure-by-Default

Die Firmware ist ab Werk Secure-by-Default. Die Einstellungen und Konfigurationen sind ab Werk so eingerichtet, dass das Produkt bestmöglichst geschützt ist.

- Die Werkseinstellungen sind dokumentiert.
- Einstellungen, welche bei der Inbetriebnahme vorgenommen werden müssen, sind dokumentiert.

Verschlüsselte Kommunikation

Der integrierte Webserver ermöglicht, für Zugriff auf das Web-Based-Management eine verschlüsselte Kommunikation zum Produkt aufzubauen.

Hinweis: Die Möglichkeit zur Verschlüsselung gilt für dieses Protokoll. Das Produkt kann weitere Protokolle aufweisen, die eine Verschlüsselung nicht unterstützen.

Die verschlüsselte Kommunikation kann über die sicheren Protokolle erfolgen:

- „Transport Layer Security“ (TLS) ermöglicht einen Aufbau zu sicheren HTTPS-Verbindungen im Netzwerk.
- „Secure Shell“ (SSH) ermöglicht den Betrieb von sicheren Shell-Verbindungen (Netzwerkdiensten) in unsicheren Netzwerken.

Update-Fähigkeit

Ein Update der Soft-/Firmware kann durch eine Erweiterung der Produkteigenschaft, Verbesserung der Soft-/Firmware oder zur Behebung einer Sicherheitslücke erfolgen.

- Das Produkt hat ab Werk keine automatische Update-Funktion.

2.5.5 Cybersecurityservice

Aktuelle Sicherheitslücken

- Informieren Sie sich und melden Sie aktuelle Sicherheitslücken.

Die folgenden Kontaktstellen können zur Information und Meldung über aktuelle Sicherheitslücken genutzt werden:

- Informationen über bekannte und aktuelle Sicherheitslücken können Sie online einsehen: „Common Vulnerabilities and Exposures (CVE)“, <https://cert.vde.com/de/advisories/vendor/wago/>.
- Für Informationen und Meldungen zu Schwachstellen von WAGO Produkten kontaktieren Sie das WAGO Product Security Incident Response Team [PSIRT](#).

Dauer des Service für Cybersecurity

- Informieren Sie sich über die Dauer des Service für Cybersecurity für Ihr Produkt.

Informationen zur Dauer des Service für Cybersecurity finden Sie auf der Produktdetailseite unter: www.wago.com/<Artikelnummer>.

3 Überblick

Bei dem Controller 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.

Der Controller kann für Anwendungen im Maschinen- und Anlagenbau sowie in der Prozessindustrie und der Gebäudetechnik eingesetzt werden.

Unter anderem verfügt der Controller über integrierte digitale und analoge Ein- und Ausgänge und zwei serielle Onboard-Schnittstellen gemäß EIA-485/RS-485.

4 Funktionen

4.1 Funktionsübersicht

Die hier aufgelisteten Funktionen sind nicht in allen Produkten enthalten.

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

Die Funktionen werden in den nachfolgenden Abschnitten beschrieben.

Systemfunktionen

-  **Benutzerverwaltung** [[▶ 23](#)]
-  **Ereignislogging** [[▶ 30](#)]
-  **Produkt- und Systemstatus** [[▶ 32](#)]
-  **Echtzeituhr** [[▶ 33](#)]
-  **Laufzeitumgebung CODESYS V3** [[▶ 34](#)]
-  **Firmware-Update** [[▶ 35](#)]
-  **Zertifikatsverwaltung** [[▶ 36](#)]
-  **Webserver** [[▶ 39](#)]
-  **Open-Source-Lizenzen** [[▶ 41](#)]
-  **WAGO Device-Access** [[▶ 41](#)]
-  **Factory-Reset** [[▶ 42](#)]

Hardwarefunktionen

-  **Betriebsartenschalter/Reset-Taster** [[▶ 42](#)]
-  **Kommunikationsschnittstelle** [[▶ 43](#)]
-  **USB-C-Service-Schnittstelle** [[▶ 43](#)]
-  **OnBoard-I/O** [[▶ 44](#)]

Konfigurationsfunktionen

-  **Web-based Management (WBM)** [[▶ 50](#)]

Netzwerkfunktionen

- Netzwerkkonfiguration
 -  **Schnittstellenkonfiguration** [[▶ 67](#)]
 -  **Hostname/Domainadressen** [[▶ 69](#)]
- Netzwerksicherheit
 -  **Firewall** [[▶ 70](#)]
 -  **IPsec** [[▶ 73](#)]
- Netzwerkdienste
 -  **DHCP-Client** [[▶ 75](#)]
 -  **SSH-Dienst** [[▶ 75](#)]

Speicherfunktionen

-  **Automount** [[▶ 76](#)]
-  **Datensicherung** [[▶ 76](#)]

Diagnosefunktionen

-  **Diagnose über Anzeigeelemente [► 77]**
-  **Diagnose über WBM oder WAGO Device Manager [► 77]**

4.2 Systemfunktionen

4.2.1 Normkonformität

Für die Produkte im Gültigkeitsbereich dieses Dokuments wird bei Erfüllung der im Abschnitt „Cybersecurity“ enthaltenen Vorgaben die Konformität nach IEC 62443-4-2 von WAGO zugesagt.

Bei Verwendung von bestimmten Funktionen oder Benutzern mit weitreichenden Rechten (z. B. „root“-User) können Modifikationen der Software vorgenommen werden, die über die zugesicherten Produktfunktionen hinausgehen.

Deshalb muss für die Verwendung die Konformitätszusage von WAGO aufgegeben werden. Die Aufgabe der Konformitätszusage kann nicht zurückgenommen werden.

Vor der Aufgabe wird ein Warnhinweis mit einer Sicherheitsabfrage ausgegeben. Mit der Aufgabe wird im Controller ein Flag dauerhaft und nicht löschar gesetzt.

Hinweis: Die Verantwortung für ein modifiziertes Produkt obliegt dem Errichter/Betreiber.

Das Setzen des Flags hat insbesondere folgende Folgen:

- Die Updatefähigkeit des Controllers ist nicht mehr garantiert.
- Die Verantwortung für die Modifikation der Firmware geht auf den Errichter/Betreiber über.
- Die Verantwortung für die Einhaltung der Security-Eigenschaften des Controllers geht auf den Errichter/Betreiber über.

Das Setzen des Flags wird angezeigt:

- Der Controller wird dauerhaft als "nicht normkonform" markiert.
- Die Markierung wird im WBM oder im WAGO Device Manager angezeigt.

Die Einstellung ist über das WBM oder über den WAGO Device Manager auf der Seite „Device“ > „Security Compliance“ möglich.

Tabelle 1: „Gerätestatus/-aktionen“ – „Security“

Parameter/Schaltfläche	Bedeutung	
[Resign IEC 62443-4-2]	Die IEC 62443-4-2 Konformitätszusage seitens WAGO wird aufgegeben. Eine Sicherheitsabfrage wird angezeigt. Die Aufgabe der Konformitätszusage kann nicht zurückgesetzt werden!	
IEC 62443-4-2 Compliance	Statusanzeige für die IEC 62443-4-2 Konformitätszusage	
	false	Die IEC 62443-4-2 Konformitätszusage wurde aufgegeben.
	true	Die IEC 62443-4-2 Konformitätszusage ist gültig.

4.2.2 Benutzerverwaltung

Der Controller bietet die Möglichkeit, Benutzerkonten mit unterschiedlichen Rollen und Rechten anzulegen, die an die betrieblichen Anforderungen angepasst sind.

Um Security-Standards zu erfüllen, muss für jeden Benutzer ein eigenes, individuelles Benutzerkonto mit eigenem Passwort vergeben werden.

Benutzerkonten können lokal angelegt, parametrisiert und verwaltet werden oder von einem zentralen LDAP-Server abgerufen werden.

Angelegte Benutzerkonten können deaktiviert werden. Sie sind dann nicht gelöscht, die Benutzer können sich aber nicht anmelden.

Die Deaktivierung/Aktivierung erfolgt durch einen Administrator mit der entsprechenden Rolle bzw. den entsprechenden Rechten.

4.2.2.1 Allgemeine Einstellungen

4.2.2.1.1 Authentifizierungshinweis

Bei der Authentifizierung wird ein einstellbarer Hinweis eingeblendet.

Die Einstellung ist durch einen Administrator mit entsprechenden Rollen und Rechten möglich.

Der Betreiber muss den Inhalt des Hinweises rechtssicher festlegen.

Ein Standardtext ist daher in der Werkseinstellung nicht vorgegeben.

Beispiele für Inhalte der Meldung:

- Die Benutzung dieses Gerätes ist nur autorisierten Personen gestattet.
- Die unbefugte Nutzung des Systems ist verboten und wird straf- und/oder zivilrechtlich geahndet.
- Die Systemnutzung wird überwacht, aufgezeichnet und geprüft.
- Die Nutzung des Systems gilt als Zustimmung zu den oben genannten Bedingungen.

Der Hinweis darf 2048 Zeichen lang sein und außer Zeilenumbrüchen keine weiteren Steuerzeichen enthalten.

4.2.2.1.2 Passwortgüte

Für alle lokalen Benutzer wird bei der Vergabe eines Passwortes die Passwortgüte überprüft. Passworte, die die Anforderungen der Passwortgüte nicht erfüllen, werden abgewiesen.

Die Werkseinstellung für die Passwortgüte entspricht den Richtlinien und Empfehlungen des BSI.

Für die Passwortgüte ist entsprechend den betrieblichen und Security-Anforderungen folgende Einstellung möglich:

- Mindestlänge des Passworts
- Mindestanzahl von Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen

Die Einstellung ist über das WBM oder über den WAGO Device Manager möglich.

Tabelle 2: „Einstellungen“ – „Accountmanagement/PasswordQuality“

Parameter	Bedeutung
Min Length	Eingabe der Mindestlänge des Passworts (6 ... 100, Werkseinstellung = 8)
Min Capital	Eingabe der Mindestanzahl von Großbuchstaben (A ... Z) (0 ... 100, Werkseinstellung = 1)
Min Lowercase	Eingabe der Mindestanzahl von Kleinbuchstaben (a ... z) (0 ... 100, Werkseinstellung = 1)
Min Digit	Eingabe der Mindestanzahl von Ziffern (0 ... 9) (0 ... 100, Werkseinstellung = 1)

Parameter	Bedeutung
Min Special	Eingabe der Mindestanzahl von Sonderzeichen () (0 ... 100, Werkseinstellung = 1)

4.2.2.1.3 Passwortänderungen

Für folgende Benutzer können Passwörter im WBM oder im WAGO Device Manager auf der Seite „Accountmanagement“ > „Basic“ geändert werden:

- Lokal verwaltete Benutzer
- Über LDAP verwaltete Benutzer
- Systembenutzer „admin“

Die Änderung erfolgt über die Schaltfläche **[Change Password]** im Bereich „Gerätestatus/Aktionen“.

In dem Änderungsdialog wird der Benutzername, das alte Passwort, das neue Passwort und die Passwortwiederholung eingegeben.

Tabelle 3: „Gerätestatus/-aktionen“ – „AccountManagement“

Schaltfläche	Bedeutung
[Change Password]	Passwort für den Benutzer „admin“ oder für angelegte Benutzer ändern. Das Passwort für den Benutzer „root“ kann über die Schaltfläche [Enable Root] geändert werden,.

4.2.2.2 Systembenutzerkonten

Im Controller sind 2 lokale „System“-Benutzerkonten fest eingerichtet.

4.2.2.2.1 Benutzerkonto „admin“

Das Benutzerkonto „admin“ ist zur Erstinbetriebnahme notwendig.

Im Auslieferungszustand ist für das Benutzerkonto „admin“ kein Passwort eingetragen. Beim ersten Login als Benutzer „admin“ muss zwingend ein Passwort vergeben werden.

Da das Benutzerkonto „admin“ anonym und nicht personalisiert ist, muss dieses nach der Erstinbetriebnahme deaktiviert werden.

Für das Benutzerkonto „admin“ ist folgende Einstellung möglich:

- Enable/Disabled

Die Aktivierung/Deaktivierung kann über das WBM oder über den WAGO Device Manager auf der Seite „Accountmanagement“ > „Basic“ im Bereich „Einstellungen“ > „SystemUser 2 (admin)“ erfolgen.

Tabelle 4: „Einstellungen“ – „SystemUser 2 (admin)“

Parameter	Bedeutung
Enabled	Einstellen, ob das Benutzerkonto „admin“ aktiviert/deaktiviert ist
	☐ Das Benutzerkonto ist nicht aktiviert.
	☒ Das Benutzerkonto ist aktiviert.

4.2.2.2.2 Benutzerkonto „root“

Das Benutzerkonto „root“ hat uneingeschränkte Rechte.

Im Auslieferungszustand ist das Benutzerkonto „root“ gesperrt und nicht nutzbar.

Für die Aktivierung muss die Konformitätszusage nach IEC 62443-4-2 aufgegeben werden.

Nur ein Administrator mit der entsprechenden Rolle bzw. den entsprechenden Rechten kann dieses Benutzerkonto aktivieren.

Bei der erstmaligen Aktivierung muss zwingend ein Passwort vergeben werden.

Da das Benutzerkonto „root“ anonym und nicht personalisiert ist und weitgehende Rechte besitzt, muss dieses Benutzerkonto nach der Verwendung deaktiviert werden.

Für das Benutzerkonto „root“ ist folgende Einstellung möglich:

- Enabled/Disabled

Die erstmalige Aktivierung kann über das WBM oder über den WAGO Device Manager auf der Seite „Accountmanagement“ > „Basic“ im Bereich „Gerätestatus/-aktionen“ erfolgen.

Tabelle 5: „Gerätestatus/-aktionen“ – „AccountManagement“

Schaltfläche	Bedeutung
[Enable Root User]	Es wird ein Dialogfenster mit Eingabefeldern für das Passwort und die Passwortwiederholung sowie einer Schaltfläche [Enable Root User] zur Aktivierung angezeigt.

Über die Schaltfläche [Enable Root User] im Bereich „Gerätestatus/-aktionen“ ist auch eine nachträgliche Passwortänderung möglich.

Jede weitere Aktivierung/Deaktivierung kann über das WBM oder über den WAGO Device Manager auf der Seite „Accountmanagement“ > „Basic“ im Bereich „Einstellungen“ > „SystemUser 1 (root)“ erfolgen.

Tabelle 6: „Einstellungen“ – „SystemUser 1 (root)“

Parameter	Bedeutung
Enabled	Einstellen, ob das Benutzerkonto „root“ aktiviert/deaktiviert ist
☐	Das Benutzerkonto ist nicht aktiviert.
☒	Das Benutzerkonto ist aktiviert.

Eine erstmalige Aktivierung über „Einstellungen“ wird mit einer Fehlermeldung abgewiesen.

4.2.2.3 Lokale Benutzerverwaltung

Lokale Benutzerrollen und Benutzerkonten werden im Controller angelegt, parametrisiert und verwaltet.

Sie sind nur für diesen Controller gültig.

Wenn einem angemeldeten Benutzer Rechte zugeordnet oder entzogen werden, so wird die Änderung erst nach einem erneuten Login des Benutzers wirksam.

4.2.2.3.1 Lokale Benutzerkonten

Für jedes lokale Benutzerkonto sind folgende Einstellungen möglich:

- Name des Benutzerkontos
- Status des Benutzerkontos (aktiviert/deaktiviert)
- Benutzerrollen (Roles - Auswahl aus Liste mit angelegten Benutzerrollen)
- Anforderung einer Passwortänderung (Force Password Change)

Die Einstellung kann über das WBM oder über den WAGO Device Manager erfolgen.

Tabelle 7: „Einstellungen“ – „User Liste“

Parameter	Bedeutung	
User Liste	Anzahl der angelegten lokalen Benutzerkonten	
User <n> (<Name>)	Für jedes angelegte lokale Benutzerkonto wird ein eigener Bereich angezeigt.	
Name	Name des Benutzerkontos eingeben;	
Enabled	Einstellen, ob das ausgewählte Benutzerkonto aktiviert/deaktiviert ist	
	☐	Das Benutzerkonto ist nicht aktiviert.
	☒	Das Benutzerkonto ist aktiviert.
Roles	Zuordnen der Benutzerrollen zum ausgewählten Benutzerkonto; Listenfeld mit möglichen Rollen und Anzeige der Anzahl der zugeordneten Benutzerrollen; Im eingeklappten Zustand werden unterhalb des Listenfelds die zugeordneten Rollen angezeigt. Im ausgeklappten Zustand wird eine Liste mit Kontrollfeldern für die verfügbaren Rollen angezeigt.	
	☐	Das Benutzerkonto besitzt die ausgewählte Rolle nicht.
	☒	Das Benutzerkonto besitzt die ausgewählte Rolle.
	<Benutzerrolle>	Einstellen, ob das Benutzerkonto die ausgewählte Rolle besitzt.
Force Password Change	Einstellen, ob beim nächsten Login das Passwort für das ausgewählte Benutzerkonto geändert werden muss	
	☐	Das Passwort muss beim nächsten Login nicht geändert werden.
	☒	Das Passwort muss beim nächsten Login geändert werden.

4.2.2.3.2 Lokale Benutzerrollen

Für jede lokale Benutzerrolle sind folgende Einstellungen möglich:

- Name der Benutzerrolle
- Berechtigungen (Permissions - Auswahl aus Liste mit vordefinierten Berechtigungen)

Die Einstellung kann über das WBM oder über den WAGO Device Manager erfolgen.

Tabelle 8: „Einstellungen“ – „UserRole Liste“

Parameter	Bedeutung	
UserRole Liste	Anzahl der angelegten lokalen Benutzerrollen	
UserRole <n> (<Name>)	Für jede angelegte lokale Benutzerrolle wird ein eigener Bereich angezeigt.	
Name	Name der Benutzerrolle eingeben (maximal 48 Zeichen); Zulässige Zeichen: Kleinbuchstaben (a ... z), Ziffern (0 ... 9), Sonderzeichen (Minus, Unterstrich)	
Permissions	Zuordnen der Berechtigungen zur ausgewählten Rolle; Listenfeld mit möglichen Berechtigungen und Anzeige der Anzahl der zugeordneten Berechtigungen; Im eingeklappten Zustand werden unterhalb des Listenfelds die zugeordneten Berechtigungen angezeigt. Im ausgeklappten Zustand wird ein Eingabefeld zur Suche und eine Liste mit Kontrollfeldern für die verfügbaren Berechtigungen angezeigt.	
	☐	Die Benutzerrolle besitzt die ausgewählte Berechtigung nicht.
	☒	Die Benutzerrolle besitzt die ausgewählte Berechtigung.

Parameter	Bedeutung	
	<Berechtigung>	Einstellen, ob die Benutzerrolle die ausgewählte Berechtigung besitzt.

4.2.2.4 Benutzerverwaltung über LDAP

LDAP-Benutzerkonten werden vom LDAP-Administrator auf einem zentralen Server angelegt, parametrisiert und verwaltet.

Sie sind gültig für alle Controller, die mit diesem Server verbunden sind, oder eine parametrierbare Teilmenge davon.

LDAP-Benutzerkonten müssen mindestens eine UID und primäre GID größer oder gleich 10000 haben, um sich am Controller zu authentifizieren. Diese Einstellung muss durch den LDAP-Administrator in der zentralen Nutzerverwaltung auf dem Server vorgenommen werden.

Wenn die Benutzerverwaltung über den LDAP-Dienst aktiviert ist, können Benutzerkonten nach zu vielen Loginfehlversuchen zeitlich begrenzt oder dauerhaft gesperrt werden. Die Anzahl der zulässigen Fehlversuche und die zeitliche Dauer der Sperre können konfiguriert werden.

Die Konfiguration sowie die Reaktivierung der Benutzerkonten erfolgen durch den LDAP-Administrator auf dem LDAP-Server.

LDAP-Benutzerinformationen werden lokal im Controller zwischengespeichert. Damit ist es möglich, dass sich LDAP-Benutzer auch bei Netzwerkausfall am Controller authentifizieren können.

Vorhandene Certificate-Revocation-Listen werden nicht genutzt, um die Gültigkeit des Gegenstellenzertifikats zu prüfen.

Für die Verbindung zwischen dem Controller und dem LDAP-Server sind folgende Einstellungen möglich:

- Enabled/Disabled
- Hosts
- Base DN
- Device Certificate
- Server CA
- Bind DN
- Auth Token

Die Einstellung kann über das WBM oder über den WAGO Device Manager erfolgen.

4.2.2.5 Benutzeranmeldung

Die Benutzeranmeldung erfolgt über einen zentralen Authentifizierungsdienst.

Alle Anmeldungen und Anmeldeversuche am Controller werden im Ereignislog gespeichert.

4.2.2.5.1 Loginfenster

Im Loginfenster werden der Hostname des Gerätes, die anfordernde Anwendung und der Authentifizierungshinweis angezeigt.

Folgende Eingaben sind erforderlich:

- Eingabe des Benutzernamens
- Eingabe des Passworts

Wenn der Administrator eine entsprechende Festlegung getroffen hat, muss beim ersten Anmelden ein neues Passwort vergeben werden.

Ein entsprechender Hinweis wird angezeigt: „Your Password is expired. A password change is required.“

Dann sind folgende Eingaben erforderlich:

- Eingabe des alten Passworts
- Eingabe des neuen Passworts
- Wiederholung des neuen Passwortes

Bei der Passwortvergabe müssen die Regeln aus Abschnitt „Passwortgüte“ beachtet werden.

Bei der Erstinbetriebnahme wird ein Fenster zur Änderung des Passwortes für den User „admin“ geöffnet mit folgendem Hinweis: „This device is in commissioning state. Please set the password for the user ‚admin‘.“

Nach einer erfolgreichen Passwortvergabe wird das Loginfenster geöffnet mit folgendem Hinweis: „Successfully updated password.“

Nach einem erfolgreichen Loginversuch wird das Loginfenster geschlossen und die Anwendung geöffnet.

Nach einem fehlgeschlagenen Loginversuch wird das Loginfenster geöffnet mit folgendem Hinweis: „Invalid username and / or password“

Nach einem fehlgeschlagenen Loginversuch kann ein neuer Versuch erst nach einer kurzen Verzögerungszeit gestartet werden, um die Angriffsgefahr zu verringern.
Es wird dann wieder das Anmeldefenster geöffnet.

4.2.2.5.2 Authentifizierungsdienst „OAuth2“

Für den Authentifizierungsdienst „OAuth2“ sind folgende, Security-relevante Einstellungen möglich:

- Gültigkeitsdauer neu ausgestellter Refresh-Tokens einstellen
- Gültigkeitsdauer neu ausgestellter Access-Tokens einstellen
- Gültigkeitsdauer neu ausgestellter Authorization-Codes einstellen
- „Silent Mode“ aktivieren/deaktivieren
- sämtliche bisher ausgestellte Tokens invalidieren
- ein bestimmtes Token invalidieren

Die Einstellungen für die Gültigkeitsdauer und den „Silent Mode“ können im WBM oder im WAGO Dievice Manager auf der Seite „OAuth2Server“ in der Gruppe „OAuth2Server“ erfolgen.

Tabelle 9: „Einstellungen“ – „OAuth2Server“

Parameter	Bedeutung
Auth Code Lifetime	Eingabe der Gültigkeitsdauer neu ausgestellter Authorization-Codes (Werkseinstellung = 60 s)
Access Token Lifetime	Eingabe der Gültigkeitsdauer neu ausgestellter Accesstokens (Werkseinstellung = 28800 s)
Refresh Token Lifetime	Eingabe der Gültigkeitsdauer neu ausgestellter Refreshtokens (Werkseinstellung = 2592000 s)

Parameter	Bedeutung	
Silent Mode Enabled	Einstellung, ob die Anzeige im Login-Fenster auf die zum Login notwendigen Felder reduziert wird (Silent Mode).	
	☐	Anzeige ist nicht reduziert (Werkseinstellung).
	☒	Anzeige ist auf notwendige Login-Felder reduziert.

Wenn der „Silent Mode“ aktiviert ist, werden im Login-Formular des Authentifizierungsdienstes ausschließlich die zum Login nötigen Input-Felder angezeigt und keine zusätzlichen Informationen über das Gerät.

Das Invalidieren von Tokens kann z. B. im Problemfall durchgeführt werden, wenn der Verdacht besteht, dass ein Token entwendet, bzw. anderswo benutzt wurde. Um das Invalidieren nur für ein bestimmtes Token durchzuführen, muss dieses bekannt sein (z. B. durch Auslesen aus dem Netzwerkverkehr).

Die Invalidierung kann im WBM oder im WAGO Device Manager auf der Seite „OAuth2Server“ im Bereich „Gerätestatus/-aktionen“ erfolgen.

Tabelle 10: „Gerätestatus/-aktionen“ – „OAuth2Server“

Schaltfläche	Bedeutung
[Revoke All Tokens]	Invalidiert sämtliche bisher ausgestellte Token
[Revoke Token]	Invalidiert ein bestimmtes Token In einem Popup-Fenster kann der Name des Tokens eingegeben werden. Die Invalidierung wird mit den Klicks der Schaltfläche [Revoke Token] bestätigt.

4.2.3 Ereignislogging

Das System enthält einen Logdienst. Der Logdienst protokolliert die Systemereignisse als Lognachrichten.

Unter Anderem werden folgende Ereignisse geloggt:

- Bedienung des Betriebsartenschalters und des Resettasters
- Anmeldungen und Anmeldeversuche am Controller
- Schreibzugriffe und Methodenaufrufe über WDX

Aus dem Ereignisprotokoll ist ersichtlich, welcher angemeldete Benutzer wann und welche Änderungen durchgeführt hat.

Jede Lognachricht enthält:

- Die Uhrzeit
- Den Komponentennamen
- Das Loglevel
- Und die Lognachricht

Die Logmeldungen sind hier nach folgendem Schema aufgebaut:

1. Zeile: „Uhrzeit # Komponentename # Loglevel“
2. Zeile: „Lognachricht“

Beispiel für Logeinträge:

„Tue Sep 02 2025 09:10:09 GMT+0200 (Mittleuropäische Sommerzeit) # xxx.service [nnn] # Information(6)“
„OMS position: STOP“

„Tue Sep 02 2025 09:10:26 GMT+0200 (Mittleuropäische Sommerzeit) # xxx.service [nnn] # Information(6)“
 „OMS position: RUN“

Das Ereignisprotokoll des Controllers wird im WBM und WAGO Device Manager über den Menübandeintrag „Geräte-Log“ angezeigt.

Die Einstellungen für das Ereignislogging erfolgen im WBM und WAGO Device Manager auf den Seiten „Logging“ bzw. „RemoteLogging“ (siehe nachfolgende Abschnitte).

Um ein nachvollziehbares Ereignisprotokoll (Auditlog) zu erhalten, müssen die Zeitstempel dem realen Zeitpunkt entsprechen. Dazu müssen die Uhrzeit und die Zeitzone des Controllers passend eingestellt werden.

Die entsprechenden Einstellungen sind im Abschnitt [🔗 Echtzeituhr \[► 33\]](#) beschrieben.

4.2.3.1 Interner Log-Speicher (Logging)

Die Größe des Log-Speichers muss bei der Inbetriebnahme an die betrieblichen Bedürfnisse angepasst werden.

Einstellbar sind

- Der minimale Log-Level
- Die maximale Log-Speichergröße

Wenn die konfigurierte maximale Größe überschritten wird, dann werden die ältesten Meldungen verworfen.

Die Anpassung für das Logging kann im WBM oder im WAGO Device Manager unter „Einstellungen“ auf der Seite „Logging“ durchgeführt werden.

Tabelle 11: „Einstellungen“ – „Logging“

Parameter	Bedeutung	
Min Log Level	Minimalen Log-Level auswählen;	
	Error	Nur Fehlermeldungen werden geloggt.
	Warning	Warnungen und Fehlermeldungen werden geloggt.
	Notice	Hinweise, Warnungen und Fehlermeldungen werden geloggt.
	Informational	Informationen, Hinweise, Warnungen und Fehlermeldungen werden geloggt; Werkseinstellung
	Debug	Alle Ereignisse und Meldungen werden geloggt.
Disk Usage Limit	Maximale Größe des Logspeichers; (Werkseinstellung: 50 MiB)	

Unter „Gerätestatus/-aktionen“ wird die aktuelle Größe des Logspeichers angezeigt.

4.2.3.2 Externer Log-Server (Remote Logging)

Das Logsystem in der Firmware erkennt keine Manipulationen der Logmeldungen. Wenn Anforderungen an den Schutz (Veränderung/Löschung/Verlust) der Logging-Daten bestehen, so können die Logging-Daten per Remote-Logging an einen zentralen Logserver gesendet werden, der diese Anforderung sicherstellt.

Die Speicherung der Logdaten auf einem zentralen Logserver ermöglicht die Sicherung von größeren Datenmengen und die Analyse von Logdaten (Intrusion Detection System, Security Information and Event Management usw.).

Die Anpassung für die Remotespeicherung kann im WBM oder im WAGO Device Manager unter „Einstellungen“ auf der Seite „RemoteLogging“ durchgeführt werden.

Tabelle 12: „Einstellungen“ – „RsyslogClientConfig 1“

Parameter	Bedeutung	
Enabled	Remote-Logging aktivieren/deaktivieren	
	☐	Remote-Logging ist nicht aktiv.
	☒	Remote-Logging ist aktiv.
Target	Zieladresse des Remote-Logging-Servers	
Port	Zielport des Remote-Logging-Servers	
Transport Protocol	Protokoll auswählen	
	UDP	UDP ist aktiv.
	TCP	TCP ist aktiv.
Device Certificate	Geräte-Zertifikat auswählen; Dieses Auswahlfeld ist nur aktiv, wenn Protokoll TCP aktiv ist.	
CA Certificate	CA-Zertifikat auswählen; Dieses Auswahlfeld ist nur aktiv, wenn Protokoll TCP aktiv ist.	
Server TLS Enabled	Server TLS aktivieren/deaktivieren	
	☐	Server TLS ist nicht aktiv.
	☒	Server TLS ist aktiv.
Server TLS Authentication	Authentifikationsmethode auswählen; Dieses Auswahlfeld ist nur aktiv, wenn Server TLS aktiv ist.	
	NoAuthentication	No Server authentication
	Fingerprint	Authenticate Server by certificate fingerprint
	SubjectAlternativeName	Authenticate Server by certificate subject alternative name (common name)
Server Certificate Fingerprint Hash Algorithm	Hashalgorithmus auswählen; Dieses Auswahlfeld ist nur aktiv, wenn Server TLS aktiv ist und als Authentifikationsmethode „Fingerprint“ ausgewählt ist.	
	SHA1	SHA1 ist aktiv.
	SHA256	SHA256 ist aktiv.
Server Certificate Fingerprint	Fingerprint-Zertifikat eingeben Dieses Eingabefeld ist nur aktiv, wenn Server TLS aktiv ist und als Authentifikationsmethode „Fingerprint“ ausgewählt ist.	

4.2.4 Produkt- und Systemstatus

Der Produkt- und Systemstatus wird auf der WBM-Seite „Information“ angezeigt:

Mit der Schaltfläche **[Calculate Config Checksum]** wird die Berechnung der Prüfsumme über die Konfiguration gestartet. Nach der Berechnung wird die Prüfsumme in einem separaten Fenster angezeigt.

Die Produkteigenschaften werden im Bereich „Gerätestatus/-aktionen“ in der Gruppe „Identity“ angezeigt:

Tabelle 13: „Gerätestatus/-aktionen“ – „Identity“

Parameter	Bedeutung
Ordernumber	Bestellnummer des Produktes
Description	Bezeichnung des Produktes
Serial Number (UII)	Eindeutige Identifikationsnummer des Produktes

Die Produktversionen werden im Bereich „Gerätestatus/-aktionen“ in der Gruppe „Versionen“ angezeigt:

Tabelle 14: „Gerätestatus/-aktionen“ – „Version“

Parameter	Bedeutung
Firmware Version	Firmwarestand
Software Release Index	Softwarestand
Hardware Release Index	Hardwarestand

4.2.5 Echtzeituhr

Um ein nachvollziehbares Ereignisprotokoll (Auditlog) zu erhalten, müssen die Zeitstempel dem realen Zeitpunkt entsprechen. Dazu müssen die Uhrzeit und die Zeitzone eingestellt werden.

Für die Verwendung von Zertifikaten ist die entsprechende Einstellung ebenfalls erforderlich.

Um die Uhrzeit für Zeitstempel auf dem Gerät fortwährend aktuell zu halten, muss die Synchronisierung der Systemzeit mittels Zeitserver (z. B. NTP) aktiviert werden. In der Werkseinstellung ist NTP nicht aktiv.

NTP ist ein unsicheres Protokoll (Keine Authentifizierung und Autorisierung notwendig). Daher muss das Netzwerk bei der Verwendung von NTP entsprechend abgesichert werden, damit es nicht zur Verfälschung der Zeiteinstellungen auf dem Controller kommen kann.

4.2.5.1 Anzeige/Manuelle Einstellung

Die Zeitzone kann im WBM oder im WAGO Device-Manager auf der Seite „SystemTime“ im Bereich „Einstellungen“ ausgewählt werden.

Tabelle 15: „Einstellungen“ – „Timezone“

Parameter	Bedeutung
Timezone	Zeitzone auswählen; Die Liste enthält verschieden Orte bzw. Hauptstädte. Mit der Auswahl werden die richtigen Zeitzoneneinstellungen übernommen.

Das aktuelle Datum und die aktuelle Uhrzeit (UTC und lokal) des Systems werden im WBM oder im WAGO Device-Manager auf der Seite „SystemTime“ im Bereich „Gerätestatus/-aktionen“ angezeigt. Wenn kein Zeitserver verfügbar ist, können Datum und Uhrzeit manuell eingestellt werden.

UTC

Tabelle 16: „Gerätestatus/-aktionen“ – „UTC“

Parameter	Bedeutung
System Time (UTC)	GMT-Datum und -Uhrzeit
	[Ändern] Öffnet einen Dialog zur Eingabe von Datum und Uhrzeit.

Local Device Time

Tabelle 17: „Gerätestatus/-aktionen“ – „Local Device Time“

Parameter	Bedeutung
System Time (locale device time)	Lokales Datum und lokale Uhrzeit
	[Ändern] Öffnet einen Dialog zur Eingabe von Datum und Uhrzeit.

4.2.5.2 Automatische Einstellung

Tabelle 18: „Einstellungen“ – „NTPClient“

Parameter	Bedeutung	
Enabled	Automatische Aktualisierung der Uhrzeit aktivieren/deaktivieren;	
	☐	Die Aktualisierung der Uhrzeit ist deaktiviert; Werkseinstellung
	☒	Die Aktualisierung der Uhrzeit ist aktiviert.
Configured Time Server	IP-Adressen der Zeitserver eingeben; Es sind maximal 4 Zeitserver in einer kommaseparierten Liste möglich.	
Configured Pools	IP-Adressen der Time-Pools eingeben; Es sind maximal 4 Time-Pools in einer kommaseparierten Liste möglich.	

4.2.6 Laufzeitumgebung CODESYS V3

Hinweis

CODESYS V3-Dokumentation lesen!

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

Hinweis

Nicht benötigte Ports und Dienste schließen!

Durch geöffnete Ports können Unbefugte Zugriff auf Ihr Automatisierungssystem erhalten.

1. Um die Gefahr von Cyberangriffen zu verringern und damit die Cyber-Security zu erhöhen, schließen Sie alle nicht von Ihrer Applikation benötigten Ports und Dienste in den Steuerungskomponenten.
2. Öffnen Sie die Ports und Dienste nur für die Dauer der Inbetriebnahme bzw. Konfiguration.

4.2.6.1 Speicherbereiche unter CODESYS V3

4.2.6.1.1 Programm- und Datenspeicher

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

4.2.6.1.2 Merkerbereich (Memory) und Retain-Bereich

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

4.2.6.2 CODESYS Web-Visualisierung

Die CODESYS Web-Visualisierung kann mit „https://<ip-adresse>/webvisu/webvisu.htm“ aufgerufen werden.

Aus Sicherheitsgründen ist der Port des CODESYS Webservers (Port 58080) nicht direkt ansprechbar, sondern wird über den zentralen Webserver umgeleitet.

4.2.6.3 Security-Einstellungen in CODESYS

Einige Security-relevante Einstellungen können nicht im Controller erfolgen, sondern müssen in der CODESYS-Entwicklungsumgebung vorgenommen werden.

4.2.6.3.1 Sichere Kommunikation zwischen Entwicklungsumgebung und Steuerung

Die Kommunikation zwischen der CODESYS Entwicklungsumgebung und der Steuerung erfolgt im Auslieferungszustand unverschlüsselt und muss abgesichert werden.

Durch Konfigurationsänderungen, wie z. B. das Hinzufügen von Zertifikaten und das Erzwingen der Verschlüsselung, kann die Kommunikation zwischen Entwicklungsumgebung und Steuerung abgesichert werden.

Die Einstellungen sind nicht im WBM oder im WAGO Device Manager möglich, sondern erfolgen in CODESYS.

Weitere Informationen hierzu finden Sie in der Onlinehilfe zu CODESYS unter „Kommunikation verschlüsseln, Security-Einstellungen verändern“.

Eine physikalische Absicherung ist durch den Einsatz in einer gesicherten Umgebung oder durch die sichere Kommunikation via VPN möglich.

4.2.6.3.2 Integrität der übertragenen Projektdateien

Know-how-Schutz und Kopierschutz einer Bootapplikation können mit Hilfe einer steuerungsspezifischen Lizenzverwaltung und einer entsprechenden Einstellung in den Objekteigenschaften der Applikation erreicht werden.

Der Downloadcode und die Bootapplikation können verschlüsselt und signiert werden.

Die Einstellungen sind nicht im WBM oder im WAGO Device Manager möglich, sondern erfolgen in CODESYS.

Weitere Informationen hierzu finden Sie in der Onlinehilfe zu CODESYS unter „Applikation schützen“.

4.2.7 Firmware-Update

Das Gerät kann über das integrierte WBM oder über die Software „WAGO Device Manager“ aktualisiert werden.

Das Update erfolgt über ein sogenanntes Updatebundle. Dabei handelt es sich um eine Datei, die alles enthält, was im Rahmen des Updates aktualisiert wird.

Während des Updatevorgangs darf das Gerät nicht ausgeschaltet werden, da sonst die Funktionsfähigkeit des Gerätes nicht mehr gewährleistet werden kann.

Beim Firmware-Update wird das Updatebundle auf das Gerät kopiert und auf Kompatibilität, Integrität und Authentizität geprüft.

Anschließend wird die Systemaktualisierung angestoßen.

Während des Firmware-Updates blinkt die „SYS“ LED in den Farben rot/grün abwechselnd.

Beim Firmware-Update bleiben die Konfigurationseinstellungen erhalten, sofern diese weiterhin kompatibel sind.

Wichtige Ereignisse des Firmwareupdates (u. a. Start, Ende, ggf. Fehlerursachen) werden im Ereignislog erfasst.

Wenn es beim Firmware-Update zu einem Fehler kommt, wird ein Rollback durchgeführt in den Gerätezustand vor dem Update.

4.2.7.1 Signaturen und Zertifikate für Updatebundle

Das Updatebundle ist durch digitale Signaturen geschützt, so dass die Authentizität und die Integrität des Updatebundles sichergestellt sind:

- Authentizität - es ist sichergestellt, dass das Updatebundle von demjenigen stammt, der angegeben hat, dass er es erstellt hat (z. B. von WAGO).
- Integrität - es ist sichergestellt, dass das Updatebundle auf dem Transportweg nicht verändert wurde.

In der Werkseinstellung sind die Signaturen für diese Prüfung so eingestellt, dass nur Updatebundles akzeptiert werden, die WAGO erstellt hat.

Für einen sicheren Betrieb des Geräts empfiehlt WAGO, die Werkseinstellung beizubehalten und nicht zu verändern.

Änderungen erfolgen auf eigene Gefahr, WAGO übernimmt in diesen Fällen keine Haftung!

Besteht dennoch die Anforderung für Änderungen, z. B. um Updatebundles oder Firmwareversionen einzusetzen, die nicht von WAGO stammen, dann sind folgende Einstellungen möglich:

- Bundle - Zertifikat, das zur Prüfung des Updatebundle als Ganzes verwendet wird
- Firmware - Zertifikat, das zur Prüfung der im Updatebundle enthaltenen Firmware genutzt wird

Die Einstellung ist über das WBM oder über den WAGO Device Manager möglich.

4.2.8 Zertifikatsverwaltung

Beim Hochladen von Gerätezertifikaten wird die Schlüssellänge bzw. der Parameter der EC-Kurve mit den Mindestanforderungen des BSI-TR-02102-2 verglichen.

Die Mindestanforderungen sind:

- RSA-Schlüssellänge:
 - 2048 bit (TPM und Software)
 - 4096 bit (nur Software)
- Parameter der EC-Kurve:
 - secp256r1 (== prime256v1)
 - secp384r1
 - secp521r1

Es wird eine RSA-Schlüssellänge von 2048 bit akzeptiert, da der aktuelle TPM2 (gemäß der TPM-Spezifikation) nur einen 2048bit-RSA-Schlüssel unterstützt.

Gerätezertifikate, die nicht den oben dargestellten Anforderungen entsprechen, können nicht generiert werden bzw. werden beim Hochladen mit einer Fehlermeldung abgewiesen.

4.2.8.1 Truststore

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

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).

Tabelle 19: „Einstellungen“ – „CertStore/CA“

Parameter	Bedeutung	
Trust Public	Festlegung, ob öffentlich vertrauten Zertifikaten vertraut wird	
	☐	Öffentlich vertrauten Zertifikaten wird nicht vertraut.
	☒	Öffentlich vertrauten Zertifikaten wird vertraut.

Tabelle 20: „Einstellungen“ – „CACertificate Liste“

Parameter	Bedeutung	
CACertificate Liste	Anzahl der konfigurierten CA-Zertifikate	
CACertificate <n>	Für jedes CA-Zertifikat wird eine eigene Gruppe angezeigt.	
Certificate	Hinzufügen oder Entfernen eines CA-Zertifikats	
	Nicht gesetzt	Es wurde noch kein CA-Zertifikat hinzugefügt.
	<Zertifikatsname>	Name des hinzugefügten CA-Zertifikats
	Auswählen	Herunterladen eines CA-Zertifikats vom Rechner
	Datei auf Gerät bereinigen	Entfernen des CA-Zertifikats vom Controller
Comment	Eingabe eines Kommentars, welcher als Zertifikatsname verwendet wird	
Trusted	Einstellung, ob dem CA-Zertifikat vertraut wird	
	☐	Dem CA-Zertifikat wird nicht vertraut.
	☒	Dem CA-Zertifikat wird vertraut.

Tabelle 21: „Einstellungen“ – „CertificateRevocationList Liste“

Parameter	Bedeutung
CertificateRevocationList Liste	Anzahl der konfigurierten Listen
CertificateRevocationList <n>	Für jede CertificateRevocationList wird eine eigene Gruppe angezeigt.
URL	Eingabe der URL zur Liste

Tabelle 22: „Gerätestatus/-aktionen“ – „CertificateRevocationList Liste“

Parameter	Bedeutung
CertificateRevocationList Liste	Anzahl der konfigurierten Listen
CertificateRevocationList <n>	Für jede CertificateRevocationList wird eine eigene Gruppe angezeigt.
Expiration	Ablaufdatum der Liste; Wenn die Liste nicht gefunden wird oder nicht heruntergeladen werden kann, wird „leer“ angezeigt.

4.2.8.2 Gerätezertifikate

Tabelle 23: „Einstellungen“ – „DeviceCertificate Liste“

Parameter	Bedeutung	
DeviceCertificate Liste	Anzahl der Gerätezertifikate	
DeviceCertificate <n>	Für jedes Zertifikat wird ein eigener Bereich angezeigt.	
Certificate	Hinzufügen oder Entfernen einer Gerätezertifikatsdatei	
	Nicht gesetzt	Es wurde noch keine Gerätezertifikatsdatei hinzugefügt.
	<Zertifikatsname>	Name der hinzugefügten Gerätezertifikatsdatei
	Auswählen	Herunterladen einer Gerätezertifikatsdatei vom Rechner
	Datei auf Gerät bereinigen	Entfernen der Gerätezertifikatsdatei vom Controller
Comment	Eingabe eines Kommentars, welcher als Zertifikatsname verwendet wird	
Private Key	Hinzufügen oder Entfernen einer zugehörigen privaten Schlüsseldatei	
	Nicht gesetzt	Es wurde noch keine Schlüsseldatei hinzugefügt.
	<Schlüssel>	Name der hinzugefügten Schlüsseldatei
	Auswählen	Herunterladen einer Schlüsseldatei vom Rechner
	Datei auf Gerät bereinigen	Entfernen der Schlüsseldatei vom Controller
Automatic Renewal	Einstellung, ob das Zertifikat automatisch erneuert wird	
	☐	Das Zertifikat wird nicht automatisch erneuert.
	☒	Das Zertifikat wird automatisch erneuert.

Tabelle 24: „Einstellungen“ – „CertStore/EnrollmentServer“

Parameter	Bedeutung	
Host	Eingabe des Hostnamens des Enrollment-Servers	
Auth User	Eingabe des Benutzernamens für die Verbindung zum Enrollment-Server	
Auth Password	Eingabe des Passwortes für die Verbindung zum Enrollment-Server	
Verbose	Einstellung, ob erweiterte Informationen über die Verbindung protokolliert werden	
	☐	Erweiterte Informationen werden nicht protokolliert.
	☒	Erweiterte Informationen werden protokolliert.
Verify Host	Einstellung, ob der Hostname verifiziert wird	
	☐	Der Hostname wird nicht verifiziert.
	☒	Der Hostname wird verifiziert.
CA Certificate	Auswahl des CA-Zertifikates für die Verifizierung	

Tabelle 25: „Gerätestatus/-aktionen“ – „CertStore/Device“

Parameter	Bedeutung	
CertStore/Device	[Create Certificate]	Ein Zertifikat auf dem Gerät erzeugen.
	[Create Certificate With Enrollment]	Ein Zertifikat auf dem Gerät erzeugen, das optional durch den Enrollment-Server signiert und/oder upgedated werden kann.

Tabelle 26: „Gerätestatus/-aktionen“ – „DeviceCertificate Liste“

Parameter	Bedeutung	
DeviceCertificate Liste	Anzahl der auf dem Gerät erzeugten Zertifikate	
DeviceCertificate <n> (<Name>)	Für jedes Zertifikat wird eine eigene Zeile angezeigt.	
	[Create Signing Request]	Erzeugen einer Textdatei, die zur Signierung verwendet werden kann.

Tabelle 27: „Gerätestatus/-aktionen“ – „IdentityCertificate <n>“

Parameter	Bedeutung	
IdentityCertificate <n> (Factory provided device identity)	Für jedes Identitätszertifikat wird ein eigener Bereich angezeigt.	
Certificate	Größe der Zertifikatsdatei	
		Download der Zertifikatsdatei
	Wenn keine Datei vorhanden ist, wird „leer“ angezeigt.	

4.2.9 Webserver

Die Firmware enthält als Webserver den Lighttpd-Webserver.

Die Konfiguration des Webserver enthält diverse Sicherheitsfeatures. Eigenmächtige Änderungen der Konfiguration durch den Anwender können zu einer eingeschränkten Sicherheit führen.

Die Standardeinstellung des Controllers ermöglicht eine starke Verschlüsselung, nutzt aber nur einfache Authentifizierungsverfahren. Da die Authentifizierung für alle sicheren Kommunikationskanäle eine zentrale Rolle spielt, ist dringend angeraten, eine sicherere Authentifizierung durchzuführen. Basis der Authentifizierung bildet das auf dem Controller gespeicherte Sicherheitszertifikat.

Im Auslieferungszustand verwendet der Controller ein zufällig generiertes Sicherheitszertifikat im x509-Format (Defaultzertifikat). Um eine sicherere Authentifizierung zu ermöglichen, muss dieses Defaultzertifikat durch ein spezifisches Zertifikat für das individuelle Gerät ersetzt werden.

Dazu muss ein entsprechendes Zertifikat über den Truststore auf das Gerät geladen werden oder ein im Gerät erzeugtes Device-Zertifikat verwendet werden.

Anschließend muss der Webserver so konfiguriert werden, dass dieses Zertifikat verwendet wird.

Der Webserver kann damit entsprechend den Security-Anforderungen sicher betrieben werden.

Die Einstellungen sind über das WBM oder den WAGO Device Manager möglich.

Tabelle 28: „Einstellungen“ – „Webserver“

Parameter	Bedeutung	
Default Application	Auswahl der Applikation, die bei alleiniger Eingabe der IP-Adresse des Produktes angezeigt wird	
	Web-based Management	Das Web-based Management wird angezeigt.
	Web Visualization	Die Webvisualisierung wird angezeigt.
Server Certificate	Auswahl des Serverzertifikats für die Authentifizierung aus einer Liste von auf dem Produkt gespeicherten Zertifikaten	

4.2.9.1 CORS-Policy

Die CORS-Policy regelt, für welche Browser-Anwendung der Cross-Origin-Zugriff auf die REST-API des Controllers zulässig ist.

Die Einstellung ist über das WBM oder über den WAGO Device Manager auf der Seite „System“ > „Webserver“ möglich.

Tabelle 29: „Einstellungen“ – „WebserverApplication <n>“

Parameter	Bedeutung
Use Separated Ports	Einstellen, ob für die ausgewählte Webserver-Applikation getrennte Ports verwendet werden. Dieses Kontrollfeld ist nur für die Webserver-Applikation 2 (Web Visualization) sichtbar und aktiv.
	☐ Es werden keine getrennten Ports für die Webvisualisierung verwendet.
	☒ Es werden getrennte Ports für die Webvisualisierung verwendet. Die Portnummern sind einstellbar.
HTTP Port	Port-Nummer für den HTTP-Port eingeben. Dieses Eingabefeld ist nur für die Webserver-Applikation 2 (Web Visualization) sichtbar und aktiv, wenn getrennte Ports verwendet werden.
HTTPS Port	Port-Nummer für den HTTPS-Port eingeben. Dieses Eingabefeld ist nur für die Webserver-Applikation 2 (Web Visualization) sichtbar und aktiv, wenn getrennte Ports verwendet werden.
CORS Policy	Auswählen, von welchen Origins „Cross Origin“-Zugriffe auf die REST-API durchgeführt werden dürfen. Dieses Auswahlfeld ist nur für die Webserver-Applikationen 2 und 3 (WAGO Auth-Service und WAGO Device Acces) sichtbar und aktiv.
	Allow all Von allen Origins dürfen „Cross Origin“-Zugriffe auf die REST-API durchgeführt werden.
	Allow all origins and null Zusätzlich zu allen normalen Origins ist auch „null“ als Wert erlaubt, was manche Browser verwenden, um zu kennzeichnen, dass die Webseite von einem lokalen Dateisystem gehostet wird.
	Allow origins from whitelist Es soll nur von den Origins auf die REST-API zugegriffen werden, die in der Whitelist erfasst sind. Achtung: Bei dieser Einstellung ist es zwingend erforderlich, dass die Origin Ihrer Anwendung in die Whitelist eingetragen wird, sonst wird der Browser den Zugriff auf die REST-API verhindern.
	None (leer) Der Webserver weist den Browser an, gar keine „Cross Origin“-Zugriffe durchzuführen.

Für die CORS-Policy sind ggf. weitere Einstellungen möglich.

Tabelle 30: „Einstellungen“ – „WebserverCORSPolicy <n>“

Parameter	Bedeutung
Name	Name der CORS-Policy (fest eingestellt)
Max Age	Maximale Lebensdauer der CORS-Policy (fest eingestellt)
Allowed Origins	Origins der Anwendungen als kommaseparierte Liste eintragen, die einen „Cross Origin“-Zugriff auf die REST-API durchführen dürfen. Dieses Eingabefeld ist nur für die CORS-Policy „Allow origins from whitelist“ sichtbar und aktiv.

4.2.10 Open-Source-Lizenzen

Tabelle 31: „Gerätestatus/-aktionen“ – „FOSSModule Liste“

Parameter	Bedeutung
FOSSModule Liste	Anzahl der vorhandenen FOSS-Module
FOSSModule <n> (<Name>)	Für jeden Listeneintrag wird ein eigener Bereich angezeigt.
Name	Name des ausgewählten FOSS-Moduls
Version	Version des ausgewählten FOSS-Moduls
Vendor	Ersteller des ausgewählten FOSS-Moduls
License Info	Größe des ausgewählten FOSS-Moduls und Download-Schaltfläche
	 Herunterladen der Lizenzinformation als Textdatei.

4.2.11 WAGO Device-Access

WAGO Device Access (WDA) ist ein zentraler Dienst im System, der den Zugriff auf die Gerätekonfiguration und deren Einstellungen erlaubt.

Der Dienst stellt eine REST-API über HTTP bereit. Die WDA-REST-API ist unter der Adresse „https://<IP>/wda“ oder „https://<Hostname des Controllers>/wda“ erreichbar.

Eine englischsprachige Onlinedokumentation passend zur installierten Version ist unter der Adresse „https://<IP>/openapi/wda.openapi.html“ oder „https://<Hostname des Controllers>/openapi/wda.openapi.html“ verfügbar. Die Onlinedokumentation kann über die Adresszeile des Internetbrowsers des angeschlossenen PCs aufgerufen werden.

4.2.11.1 Geräte-Scan

Bei einem Geräte-Scan liefert der Controller folgende Geräteinformationen zurück:

- Die Artikelnummer
- Die Firmwareversion

Wenn der authentifizierungsfreie Geräte-Scan aktiviert ist, sind diese Informationen ohne Authentifizierung abfragbar.

Dies verringert die Security des Gerätes. In der Werkseinstellung wird eine Authentifizierung benötigt.

Die Einstellung ist über das WBM oder den WAGO Device-Manager auf der Seite „WAGODeviceAccess“ möglich.

Tabelle 32: „Einstellungen“ – „WAGODeviceAccess“

Parameter	Bedeutung
Allowed Unauthenticated Requests	Auswahlfeld mit möglichen Einträgen und Anzeige der aktivierten Einträge; Im eingeklappten Zustand werden unterhalb des Auswahlfelds die aktivierten Einträge angezeigt. Im ausgeklappten Zustand wird eine Liste mit Kontrollfeldern für jeden Eintrag angezeigt.
	☐ Das Scannen ist nur mit Authentifizierung möglich.
	☒ Das Scannen ist ohne Authentifizierung möglich.
	ScanDevices Einstellung, ob Geräte ohne Authentifizierung gescannt werden dürfen.

4.2.12 Factory-Reset

Hinweis

Alle Parameter und Passwörter werden überschrieben!

Mit dem Reset werden alle Parameter und Passwörter überschrieben.

Gespeicherte Boot-Projekte einschließlich vorhandener Webvisualisierungsdaten werden gelöscht.

Nachinstallierte Firmwarefunktionen werden gelöscht.

Softwarelizenzen werden gelöscht.

- Bei Rückfragen wenden Sie sich an den WAGO Support.

Der Controller kann über das WBM oder über den WAGO Device-Manager auf der Seite „System“ > „Factory Reset“ auf die Werkseinstellungen zurückgesetzt werden.

Tabelle 33: „Gerätestatus/-aktionen“ – „FactorySettings“

Schaltfläche	Bedeutung
[Reset]	Der Controller wird auf die Werkseinstellungen zurückgesetzt.

Alternativ ist ein Reset auch über den Betriebsartenschalter und den Resettaster möglich.

Die Vorgehensweise ist im Abschnitt  **Factory-Reset** [[▶ 89](#)] beschrieben.

4.3 Hardwarefunktionen

4.3.1 Betriebsartenschalter/Reset-Taster

Bedienhandlungen des Betriebsartenschalters und des Resettasters werden im Ereignislog gespeichert. Damit ist eine Nachverfolgung von unzulässigen Bedienhandlungen nach Security-Richtlinien möglich.

4.3.1.1 Betriebsartenschalter

Tabelle 34: Betriebsartenschalter

Pos.	Betätigung	Funktion
RUN	Rastend	Normalbetrieb CODESYS V3-Applikationen laufen.
STOP	Rastend	Stop Alle CODESYS V3-Applikationen sind gestoppt.
RESET	Tastend	Warmstart-Reset oder Kaltstart-Reset (Abhängig von der Betätigungsdauer)

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

Jede Betätigung des Betriebsartenschalters wird bei Erreichen einer geänderten Position im Logsystem erfasst (Ereignislogging).

Beispiel für Logeinträge zum Betriebsartenschalter:

```
Mar 10 13:29:05 wago-cc100 mcid[450]: OMS position: RUN
Mar 10 13:30:09 wago-cc100 mcid[450]: OMS position: STOP
Mar 10 13:30:11 wago-cc100 mcid[450]: OMS position: RESET
```

4.3.1.2 Reset-Taster

In Verbindung mit dem Betriebsartenschalter können weitere Funktionen ausgelöst werden.

Tabelle 35: Reset-Taster

Position Betriebsarten-schalter	Betätigungsdauer Reset-Taster	Funktion
RUN oder STOP	1 ... 8 Sekunden	Software-Reset, der Controller wird neu gestartet. 🔗 Software-Reset (Neustart) [> 89]
RESET	> 8 Sekunden	Factory-Reset, der Controller wird auf die Werkseinstellungen zurückgesetzt, alle Parameter werden gelöscht. 🔗 Factory-Reset [> 89]

Jede Betätigung des Reset-Tasters (Drücken und Loslassen) wird im Logsystem erfasst (Ereignislogging).

Beispiel für Logeinträge zum Reset-Taster:

```
Mar 10 13:30:39 wago-cc100 mcid[450]: Button RESET_ALL: PRESSED
Mar 10 13:30:39 wago-cc100 mcid[450]: Button RESET_ALL: RELEASED
```

4.3.2 Kommunikationsschnittstelle

Die Kommunikation über serielle Standardprotokolle ist unsicher und es gibt keine Protokoll-Mechanismen zur Absicherung.

Um Security-Anforderungen zu erfüllen, muss durch den Betreiber eine physikalische Absicherung erfolgen (z. B. geschützte Verlegung der Leitungen, Schutz vor unbefugtem Zutritt).

4.3.3 USB-C-Service-Schnittstelle

Die Service-Schnittstelle ist als USB-C-Schnittstelle ausgebildet und stellt eine Netzwerk-Schnittstelle mit der IP-Adresse 192.168.42.42 dar.

Die Service-Schnittstelle kann zur Konfiguration und für Servicezwecke verwendet werden.

Um Security-Anforderungen zu erfüllen, kann eine Verbindung über die Service-Schnittstelle verhindert werden, indem die Service-Schnittstelle bei Nichtgebrauch abgeschaltet wird.

** Hinweis****Aussperren möglich bei Abschaltung aller Schnittstellen!**

Wenn alle Netzwerk-Schnittstellen und die USB-C-Service-Schnittstelle abgeschaltet sind, ist das Gerät nicht mehr erreichbar.

Diese Konfiguration kann nur über ein Rücksetzen auf Werkseinstellungen aufgehoben werden.

Das Abschalten und Reaktivieren der Service-Schnittstelle erfolgt erst nach einem Geräte-neustart.

Die Einstellung ist über das WBM oder den WAGO Device Manager auf der Seite „Interfaces“ > „USB Service Interface“ möglich.

Tabelle 36: „Einstellungen“ – „USBServiceInterface“

Parameter	Bedeutung	
Enabled	USB-Service-Schnittstelle aktivieren/deaktivieren.	
	☐	Die USB-Service-Schnittstelle ist nicht aktiv.
	☒	Die USB-Service-Schnittstelle ist aktiv.

4.3.4 OnBoard-I/O

4.3.4.1 Analogeingänge AI1, AI2

Tabelle 37: Prozessabbild – Analogeingänge AI1, AI2

Eingang	Pin	E/A-Kanal	Datentyp	Beschreibung
AI1	X14.1	X14.AI1	WORD	Analogeingang 1
AI2	X14.3	X14.AI2	WORD	Analogeingang 2

Die Messbereiche der Analogeingänge sind kanalweise konfigurierbar.

Die Konfiguration erfolgt mit CODESYS oder mit dem Tool „WAGO Device Manager“.

Folgende Messbereiche sind konfigurierbar:

- 0 ... 10 V, Default-Einstellung
- -10 ... +10 V
- 0 ... 20 mA
- 4 ... 20 mA
- 3,6 ... 21 mA

4.3.4.1.1 AI 0 ... 10 V

Messwerte werden über den Datentyp WORD (16 Bit) dargestellt.

Tabelle 38: Prozessabbild – Prozesswerte AI; 0 ... 10 V; 16 Bit, WORD

Messwert	Wertebereich		
	Hex.	Dez.	Bin.
< 0 V	0x0000	0	0000.0000.0000.0000
0 V	0x0000	0	0000.0000.0000.0000
...	...	...	...
10 V	0x7FFF	32767	0111.1111.1111.1111
> 10 V	0x7FFF	32767	0111.1111.1111.1111

4.3.4.1.2 AI -10 ... 10 V

Messwerte werden über den Datentyp WORD (16 Bit) dargestellt.

Tabelle 39: Prozessabbild – Prozesswerte AI; -10 ... +10 V; 16 Bit; WORD

Messwert	Wertebereich		
	Hex.	Dez.	Bin.
< -10 V	0x8000	-32768	1000.0000.0000.0000
-10 V	0x8000	-32768	1000.0000.0000.0000
...	...	...	...
+10 V	0x7FFF	32767	0111.1111.1111.1111

Messwert	Wertebereich		
	Hex.	Dez.	Bin.
> +10 V	0x7FFF	32767	0111.1111.1111.1111

4.3.4.1.3 AI 0 ... 20 mA

Messwerte werden über den Datentyp WORD (16 Bit) dargestellt.

Tabelle 40: Prozessabbild – Prozesswerte AI; 0 ... 20 mA; 16 Bit; WORD

Messwert	Wertebereich		
	Hex.	Dez.	Bin.
< 0 mA	0x0000	0	0000.0000.0000.0000
0 mA	0x0000	0	0000.0000.0000.0000
...	...	...	...
20 mA	0x7FFF	32767	0111.1111.1111.1111
> 20 mA	0x7FFF	32767	0111.1111.1111.1111

4.3.4.1.4 AI 4 ... 20 mA

Messwerte werden über den Datentyp WORD (16 Bit) dargestellt.

Tabelle 41: Prozessabbild – Prozesswerte AI; 4 ... 20 mA; 16 Bit; WORD

Messwert	Wertebereich		
	Hex.	Dez.	Bin.
< 4 mA	0x0000	0	0000.0000.0000.0000
4 mA	0x0000	0	0000.0000.0000.0000
...	...	...	...
20 mA	0x7FFF	32767	0111.1111.1111.1111
> 20 mA	0x7FFF	32767	0111.1111.1111.1111

4.3.4.1.5 AI 3,6 ... 21 mA

Messwerte werden über den Datentyp WORD (16 Bit) dargestellt.

Tabelle 42: Prozessabbild – Prozesswerte AI; 3,6 ... 21 mA; 16 Bit; WORD

Messwert	Wertebereich		
	Hex.	Dez.	Bin.
< 3,6 mA	0xFD03	-765	1111 1101 0000 0011
3,6 mA	0xFD03	-765	1111 1101 0000 0011
...	...	...	...
21 mA	0x7FFB	32763	0111.1111.1111.1011
> 21 mA	0x7FFB	32763	0111.1111.1111.1011

4.3.4.2 Analogein-/ausgänge AIO1, AIO2

Tabelle 43: Prozessabbild – Analogein-/ausgänge AIO1, AIO2

Ein-/Ausgang	Pin	E/A-Kanal	Datentyp	Beschreibung
AIO1	X6.1	X6.AIO1	WORD	Analogein-/ausgang 1
AIO2	X6.3	X6.AIO2	WORD	Analogein-/ausgang 2

Die Messbereiche der Analogein-/ausgänge sind kanalweise konfigurierbar.

Die Konfiguration erfolgt mit CODESYS oder mit dem Tool „WAGO Device Manager“.

Folgende Messbereiche sind konfigurierbar:

- Eingänge
 - 0 ... 10 V, Default-Einstellung
 - -10 ... +10 V
 - 0 ... 20 mA
 - 4 ... 20 mA
 - 3,6 ... 21 mA
- Ausgänge
 - 0 ... 10 V
 - -10 ... +10 V
 - -12 ... +12 V
 - 0 ... 20 mA
 - 0 ... 22 mA
 - 4 ... 20 mA

4.3.4.2.1 AI 0 ... 10 V, -10 ... +10 V, 0 ... 20 mA, 4 ... 20 mA, 3,6 ... 21 mA

Wenn ein Analogeingang/-ausgang AIO1/AIO2 als Eingang konfiguriert ist, gelten die Tabellen der Prozesswerte der Analogeingänge AI1/AI2.

4.3.4.2.2 AO 0 ... 10 V

Messwerte werden über den Datentyp WORD (16 Bit) dargestellt.

Tabelle 44: Prozessabbild – Prozesswerte AO; 0 ... 10 V; 16 Bit; WORD

Messwert	Wertebereich		
	Hex.	Dez.	Bin.
0 V	0x0000	0	0000.0000.0000.0000
...	...	...	...
10 V	0x7FFF	32767	0111.1111.1111.1111

4.3.4.2.3 AO -10 ... +10 V

Messwerte werden über den Datentyp WORD (16 Bit) dargestellt.

Tabelle 45: Prozessabbild – Prozesswerte AO; -10 ... +10 V; 16 Bit; WORD

Messwert	Wertebereich		
	Hex.	Dez.	Bin.
-10 V	0x8000	-32768	1000.0000.0000.0000
...	...	...	...
+10 V	0x7FFF	32767	0111.1111.1111.1111

4.3.4.2.4 AO -12 ... +12 V

Messwerte werden über den Datentyp WORD (16 Bit) dargestellt.

Tabelle 46: Prozessabbild – Prozesswerte AO; -12 ... +12 V; 16 Bit; WORD

Messwert	Wertebereich		
	Hex.	Dez.	Bin.
-12 V	0x8000	-32768	1000.0000.0000.0000
...	...	...	...
+12 V	0x7FFF	32767	0111.1111.1111.1111

4.3.4.2.5 AO 0 ... 20 mA

Messwerte werden über den Datentyp WORD (16 Bit) dargestellt.

Tabelle 47: Prozessabbild – Prozesswerte AO; 0 ... 20 mA; 16 Bit; WORD

Messwert	Wertebereich		
	Hex.	Dez.	Bin.
0 mA	0x0000	0	0000.0000.0000.0000
...	...	...	...
20 mA	0x8000	32768	1000.0000.0000.0000

4.3.4.2.6 AO 0 ... 22 mA

Messwerte werden über den Datentyp WORD (16 Bit) dargestellt.

Tabelle 48: Prozessabbild – Prozesswerte AO; 0 ... 22 mA; 16 Bit; WORD

Messwert	Wertebereich		
	Hex.	Dez.	Bin.
0 mA	0x0000	0	0000.0000.0000.0000
...	...	...	...
22 mA	0x7FFF	32767	0111.1111.1111.1111

4.3.4.2.7 AO 4 ... 20 mA

Messwerte werden über den Datentyp WORD (16 Bit) dargestellt.

Tabelle 49: Prozessabbild – Prozesswerte AO; 4 ... 20 mA; 16 Bit; WORD

Messwert	Wertebereich		
	Hex.	Dez.	Bin.
4 mA	0x0000	0	0000.0000.0000.0000
...	...	...	...
20 mA	0x7FFF	32767	0111.1111.1111.1111

4.3.4.3 Temperatureingänge PT1+/PT1–, PT2+/PT2–

Tabelle 50: Prozessabbild – Temperatureingänge PT1+/PT1–, PT2+/PT2–

Eingang	Pin	E/A-Kanal	Datentyp	Beschreibung
PT1+	X13.1	X13.PT1+/PT1–	INT	RTD-Eingang 1
PT1–	X13.2			
PT2+	X13.3	X13.PT2+/PT2–	INT	RTD-Eingang 2
PT2–	X13.4			

Die Messbereiche der RTD-Eingänge sind kanalweise konfigurierbar.

Die Konfiguration erfolgt mit CODESYS oder mit dem Tool „WAGO Device Manager“.

Folgende Messbereiche sind konfigurierbar:

- Pt100 (–200 ... +850 °C)
- Pt200 (–200 ... +850 °C)
- Pt500 (–200 ... +850 °C)
- Pt1000 (–200 ... +850 °C), Default-Einstellung
- Ni100 (–60 ... +250 °C)
- Ni120 (–80 ... +260 °C)
- Ni1000 (TK6180) (–60 ... +250 °C)
- Ni1000 (TK5000) (–60 ... +250 °C)
- Potentiometer 0 ... 1,2 kOhm
- Potentiometer 0 ... 5 kOhm

Hardwareseitig können Widerstandswerte zwischen 450 und 4400 Ohm erfasst werden. Die Darstellung von Widerstandswerten außerhalb dieses Bereiches ist nicht definiert.

4.3.4.3.1 Pt100, Pt200, Pt500, Pt1000

Messwerte werden über den Datentyp INT (16 Bit) dargestellt.

Die Auflösung beträgt 1 Digit pro 0,1 °C.

Tabelle 51: Prozessabbild – Prozesswerte RTD; Pt100, Pt200, Pt500, Pt1000; –200 ... +850 °C; 16 Bit; INT

Messwert	Wertebereich		
	Hex.	Dez.	Bin.
< –200 °C	0xF830	–2000	1111.1000.0011.0000
–200 °C	0xF830	–2000	1111.1000.0011.0000
...	...	...	...
+850 °C	0x2134	8500	0010.0001.0011.0100
> +850 °C	0x2134	8500	0010.0001.0011.0100

4.3.4.3.2 Ni100, Ni1000 (TK6180), Ni1000 (TK5000)

Messwerte werden über den Datentyp INT (16 Bit) dargestellt.

Die Auflösung beträgt 1 Digit pro 0,1 °C.

Tabelle 52: Prozessabbild – Prozesswerte RTD; Ni100, Ni1000 (TK6180), Ni1000 (TK5000); –60 ... +250 °C; 16 Bit; INT

Messwert	Wertebereich		
	Hex.	Dez.	Bin.
< –60 °C	0xFDA8	–600	1111.1101.1010.1000
–60 °C	0xFDA8	–600	1111.1101.1010.1000
...	...	...	...
+250 °C	0x09C4	2500	0000.1001.1100.0100
> +250 °C	0x09C4	2500	0000.1001.1100.0100

4.3.4.3.3 Ni120

Messwerte werden über den Datentyp INT (16 Bit) dargestellt.

Die Auflösung beträgt 1 Digit pro 0,1 °C.

Tabelle 53: Prozessabbild – Prozesswerte RTD; Ni120; –80 ... +260 °C; 16 Bit; INT

Messwert	Wertebereich		
	Hex.	Dez.	Bin.
< –80 °C	0xFCE0	–800	1111.1100.1110.0000
–80 °C	0xFCE0	–800	1111.1100.1110.0000
...	...	...	...
+260 °C	0x0A28	2600	0000.1010.0010.1000
> +260 °C	0x0A28	2600	0000.1010.0010.1000

4.3.4.3.4 Potentiometer 0 ... 1,2 kOhm

Messwerte werden über den Datentyp INT (16 Bit) dargestellt.

Die Auflösung beträgt 1 Digit pro 0,05 Ohm.

Tabelle 54: Prozessabbild – Prozesswerte RTD; Potentiometer; 0 ... 1200 Ohm; 16 Bit; INT

Messwert	Wertebereich		
	Hex.	Dez.	Bin.
< 0 Ohm	0x0000	0	0000.0000.0000.0000
0 Ohm	0x0000	0	0000.0000.0000.0000
...	...	...	...
1200 Ohm	0x5DC0	24000	0101.1101.1100.0000
> 1200 Ohm	0x5DC0	24000	0101.1101.1100.0000

4.3.4.3.5 Potentiometer 0 ... 5 kOhm

Messwerte werden über den Datentyp INT (16 Bit) dargestellt.

Die Auflösung beträgt 1 Digit pro 0,2 Ohm.

Tabelle 55: Prozessabbild – Prozesswerte RTD; Potentiometer; 0 ... 5000 Ohm; 16 Bit; INT

Messwert	Wertebereich		
	Hex.	Dez.	Bin.
< 0 Ohm	0x0000	0	0000.0000.0000.0000
0 Ohm	0x0000	0	0000.0000.0000.0000
...	...	...	...
5000 Ohm	0x61A8	25000	0110.0001.1010.1000
> 5000 Ohm	0x61A8	25000	0110.0001.1010.1000

4.3.4.4 Digitaleingänge DI

Tabelle 56: Prozessabbild – Digitaleingänge DI1 ... DI8

Eingang	Pin	E/A-Kanal	Datentyp	Beschreibung
DI1	X12.3	X12.DI1	BOOL	Digitaleingang 1
DI2	X12.4	X12.DI2	BOOL	Digitaleingang 2
DI3	X12.5	X12.DI3	BOOL	Digitaleingang 3
DI4	X12.6	X12.DI4	BOOL	Digitaleingang 4
DI5	X12.7	X12.DI5	BOOL	Digitaleingang 5
DI6	X12.8	X12.DI6	BOOL	Digitaleingang 6
DI7	X12.9	X12.DI7	BOOL	Digitaleingang 7
DI8	X12.10	X12.DI8	BOOL	Digitaleingang 8

Messwerte werden pro Kanal über den Datentyp BOOL dargestellt.

Tabelle 57: Prozessabbild – Prozesswerte digitale Eingänge – BOOL

Messwert	Wertebereich		
	Hex.	Dez.	Bin.
0 V	---	---	FALSE
+24 V	---	---	TRUE

4.3.4.5 Digitalein-/ausgänge DIO

Tabelle 58: Prozessabbild – Digitalein-/ausgänge DIO1 ... DIO8

Ein-/Ausgang	Pin	E/A-Kanal	Datentyp	Beschreibung
DIO1	X5.3	X5.DIO1	BOOL	Digitalein-/ausgang 1
DIO2	X5.4	X5.DIO2	BOOL	Digitalein-/ausgang 2
DIO3	X5.5	X5.DIO3	BOOL	Digitalein-/ausgang 3
DIO4	X5.6	X5.DIO4	BOOL	Digitalein-/ausgang 4

Ein-/Ausgang	Pin	E/A-Kanal	Datentyp	Beschreibung
DIO5	X5.7	X5.DIO5	BOOL	Digitalein-/ausgang 5
DIO6	X5.8	X5.DIO6	BOOL	Digitalein-/ausgang 6
DIO7	X5.9	X5.DIO7	BOOL	Digitalein-/ausgang 7
DIO8	X5.10	X5.DIO8	BOOL	Digitalein-/ausgang 8

Die Konfiguration erfolgt mit CODESYS oder mit dem Tool „WAGO Device Manager“.

4.3.4.5.1 DI 0/24 V

Messwerte werden pro Kanal über den Datentyp BOOL dargestellt.

Tabelle 59: Prozessabbild – Prozesswerte digitale Eingänge – BOOL

Messwert	Wertebereich		
	Hex.	Dez.	Bin.
0 V	---	---	FALSE
+24 V	---	---	TRUE

4.3.4.5.2 DO 0/24V

Tabelle 60: Prozessabbild – Prozesswerte digitale Ausgänge – BOOL

Messwert	Wertebereich		
	Hex.	Dez.	Bin.
0 V	---	---	FALSE
+24 V	---	---	TRUE

Messwerte werden pro Kanal über den Datentyp BOOL dargestellt.

4.4 Konfigurationsfunktionen

4.4.1 Web-based Management (WBM)

Die Abbildungen in den folgenden Abschnitten sind beispielhaft und können von der tatsächlichen Ausführung der Produkte abweichen.

Die grafische Benutzeroberfläche ist wie folgt aufgebaut:

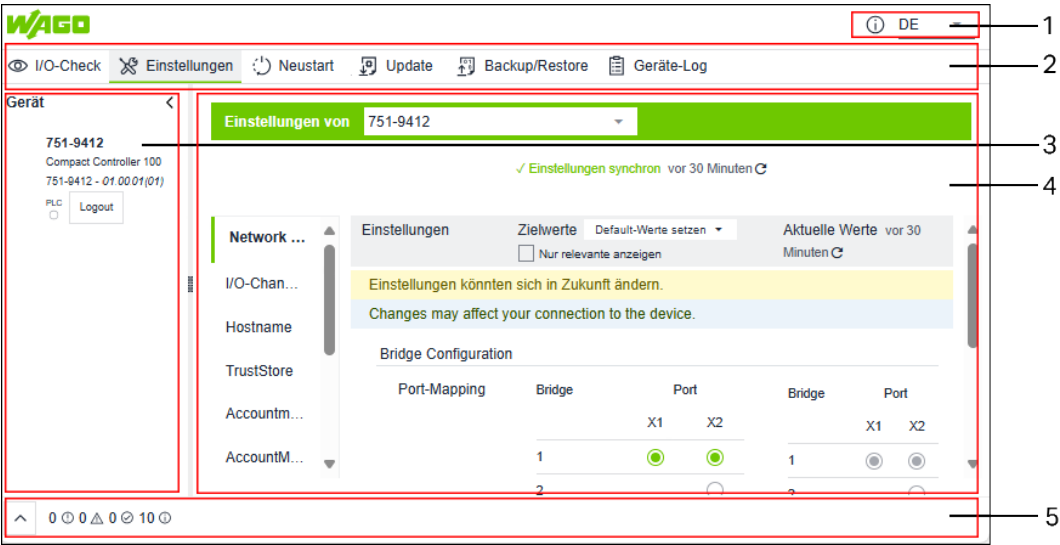


Abbildung 3: Grafische Benutzeroberfläche

4.4.1.1 Allgemeine Bedienelemente

Über die folgenden Bedienelemente werden allgemeine Einstellungen vorgenommen und Informationen zum WBM angezeigt:

Bedienelement	Beschreibung
	Zeigt allgemeine Kontakt- und Programminformationen an: WAGO und Support-Kontakt daten, WAGO Software-Lizenzbedingungen, Impressum , Datenschutz , AGB , Rechtliche Hinweise und die Programmversion des WBM
	Schaltet die Sprache der Benutzeroberfläche zwischen Deutsch, Englisch und Französisch um.

4.4.1.2 Menüband (Geräteaktionen)

Über das Menüband werden die folgenden Geräteaktionen ausgeführt:

Symbol	Funktion	Beschreibung
	I/O-Check	Öffnet die Ansicht „I/O-Check“ im Arbeitsbereich und stellt das verwendete Gerät grafisch dar. Der Status des Gerätes und der angeschlossenen Kanäle wird via LED-Anzeigen dargestellt. Per Control-Modus kann ein Verdrahtungstest durchgeführt werden.
	Einstellungen	Öffnet die Ansicht „Einstellungen“ im Arbeitsbereich. In dieser Ansicht wird die Parametrierung und Konfiguration des verwendeten Gerätes vorgenommen.
	Neustart	Öffnet die Ansicht „Neustart“ im Arbeitsbereich. In dieser Ansicht kann das verwendete Gerät neu gestartet werden.
	Firmware	Öffnet die Ansicht „Firmware“ im Arbeitsbereich. In dieser Ansicht wird die Firmware des verwendeten Gerätes angezeigt und kann gegen eine andere ersetzt werden.
	Backup/Restore	Öffnet die Ansicht „Backup/Restore“ im Arbeitsbereich. In dieser Ansicht werden Gerätedaten als Datei gesichert (Backup) oder gespeicherte Backup-Dateien in ein Gerät geladen (Restore).
	Geräte-Log	Öffnet die Ansicht „Geräte-Log“ im Arbeitsbereich. In dieser Ansicht können protokollierte Log-Einträge des Gerätes angezeigt werden.

4.4.1.3 Gerät

Im Bereich „Gerät“ wird das verbundene Gerät angezeigt.

Es werden Geräteinformationen, Verbindungs- und Statusinformationen sowie eine Schaltfläche für die Trennung der Verbindung angezeigt.

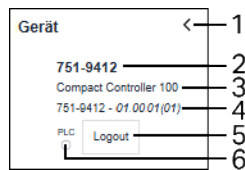


Abbildung 4: Verbundenes Gerät

Pos.	Beschreibung
1	Aus-/Einklappen der Ansicht
2	Name des Gerätes Nach dem Verbinden des Gerätes wird die Artikelnummer als Gerätenamen verwendet.
3	Artikelbezeichnung des Gerätes
4	Artikelnummer und Firmwareversion des Gerätes
5	[Logout] Schaltfläche zum Abmelden vom Gerät
6	Der Status der SPS-Applikation eines online verbundenen Gerätes wird über folgende LED-Anzeige dargestellt. PLC ☐ Keine Applikation vorhanden ☒ Applikation läuft oder Applikation im Debug ☐ Applikation gestoppt, nicht konfiguriert, im Fehlerzustand oder in unbekanntem Zustand Hinweise: • Detaillierte LED-Anzeigen, siehe Geräteansicht oder Einstellungen > Register „LEDs“. • Die Erläuterung von LED-Anzeigen und Blinkcodes finden Sie im Produkt- bzw. Funktionshandbuch zum verbundenen Gerät.

4.4.1.4 Arbeitsbereich

Der Arbeitsbereich umfasst den rechten Fensterbereich unterhalb des Menübandes. Abhängig von der im Menüband getroffenen Auswahl wird der entsprechende Inhalt zur Bearbeitung geöffnet. Umgekehrt hat eine Selektion im Arbeitsbereich keine Rückwirkung auf die Auswahl im Menüband.

Im Folgenden werden die unterschiedlichen Ansichten des Arbeitsbereiches je nach Tätigkeit beschrieben.

4.4.1.4.1 I/O-Check

Basierend auf der Geräteansicht können Verdrahtungstests für konventionelle, analoge und digitale Ein-/Ausgänge eines Gerätes durchgeführt werden, indem z. B. testweise Ausgangssignale gesetzt werden (siehe auch Gerätediagnose durchführen).

i Hinweis

Prüfung von Ein- und Ausgängen nicht für alle Geräte verfügbar

Beachten Sie, dass nicht alle Geräte eine Prüfung von Ein- und Ausgängen unterstützen. Für diese Geräte ist lediglich die Geräteansicht mit den Statusanzeigen verfügbar.

Im oberen Bereich der Ansicht „I/O-Check“ wird die verwendete Gerätehardware visuell dargestellt. Dabei zeigen die LED-Anzeigen auf der linken Seite den Status des Gerätes und die LED-Anzeigen der rechten Seite den Status der Kanäle an.

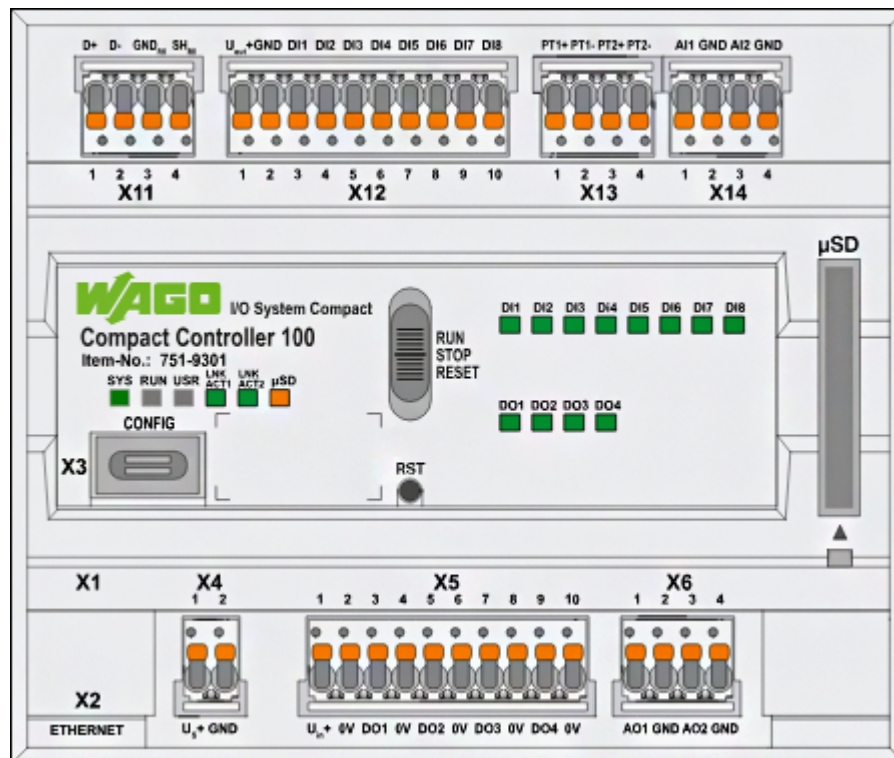


Abbildung 5: Ansicht „I/O-Check“ (Beispiel)

Statusanzeigen des Gerätes

Die Statusanzeigen der Kopfstation sind immer aktiv. Die LED-Anzeigen in der Grafik sind nicht klickbar, zeigen aber bei Mouse-Over die aktuelle Statusmeldung der Kopfstation an.

i Hinweis

Blinkcodes zeigen keine reale Frequenz

Beachten Sie, dass Blinkcodes nicht in der realen Frequenz dargestellt werden. Ausführliche Beschreibungen der Diagnosemeldungen und Blinkcodes finden Sie im Handbuch des jeweiligen Produktes.



Abbildung 6: Statusanzeige des Gerätes (Beispiel)

Statusanzeigen der Kanäle

Die Statusanzeigen für die angeschlossenen Kanäle zeigen nicht permanent, sondern nur im Monitormodus den aktuellen Status (nur lesend) der verwendeten Digitalein- und Digitalausgänge an. Der Monitormodus ist aktiv, sofern eine Onlineverbindung zum Gerät besteht.

Hinweis

LED-Status bezieht sich auf Ein/Aus-Statuswerte digitaler E/A-Kanäle

Für Diagnosekanäle setzen sich die Anzeigen der physischen LED-Anzeigen ggf. aus mehreren Statuswerten zusammen. Der hier angezeigte LED-Status bezieht sich nur auf Ein/Aus-Statuswerte mit direktem Bezug zu digitalen E/A-Kanälen.



Abbildung 7: Statusanzeige der Kanäle (Beispiel)

Durch Anklicken des Augen-Icons unter dem jeweiligen Gerät werden Tabellen mit Statuswerten zu den Kanälen der verwendeten Ein- und Ausgänge angezeigt. Die Anzeige ist umschaltbar zwischen Control- und Monitormodus.

Bedienelement	Beschreibung
	Vergrößern Vergrößert die Gerätesicht je Klick um eine Stufe.
	Verkleinern Verkleinert die Gerätesicht je Klick um eine Stufe.
	Originalgröße Zeigt die Gerätesicht in der Originalgröße an.
	Größe der angezeigten Bereiche anpassen Durch Verschieben der Trennlinie kann der Bereich zwischen Gerätesicht und Statuswerttabellen angepasst werden.
	Tabellen mit Statuswerten ausgeblendet Beim Öffnen der Ansicht „I/O-Check“ sind die Tabellen mit Statuswerten für Ein-/Ausgangskanäle zunächst ausgeblendet. Mit einem Klick auf das ausgegraute Augen-Icon werden die Tabellen unterhalb der Gerätegrafik eingeblendet.
	Tabellen mit Statuswerten eingeblendet Durch Anklicken des Augen-Icons werden die angezeigten Tabellen für die Statuskanäle wieder ausgeblendet.
	Direkt zu Einstellungen der I/O-Kanäle wechseln Springt zur Ansicht „Einstellungen“ > Register „I/O-Channels“ und in diesem Register zur ersten konfigurierbaren Kanalkomposition.
 Control-Modus	Control-Modus aktiv Bei aktivem Control-Modus werden die Kanäle für Änderungen freigeschaltet. Werte können geschrieben werden.
 Control-Modus	Monitormodus aktiv Bei deaktiviertem Control-Modus werden aktuelle Statuswerte angezeigt (nur Lesezugriff).

Es wird außerdem die Latenz angezeigt, d. h. der Aktualisierungszyklus (in s) der angezeigten Gerätewerte in Abhängigkeit von der Verbindung, Geräteauslastung oder anderen Faktoren:

Anzeige	Beschreibung
 Monitoring aktiv	Niedrige Latenz, hohe Synchronisationsrate
 Monitoring aktiv	Erhöhte Latenz, verzögerte Synchronisationsrate

Anzeige	Beschreibung
 Verbindung instabil	Hohe Latenz, instabile Verbindung

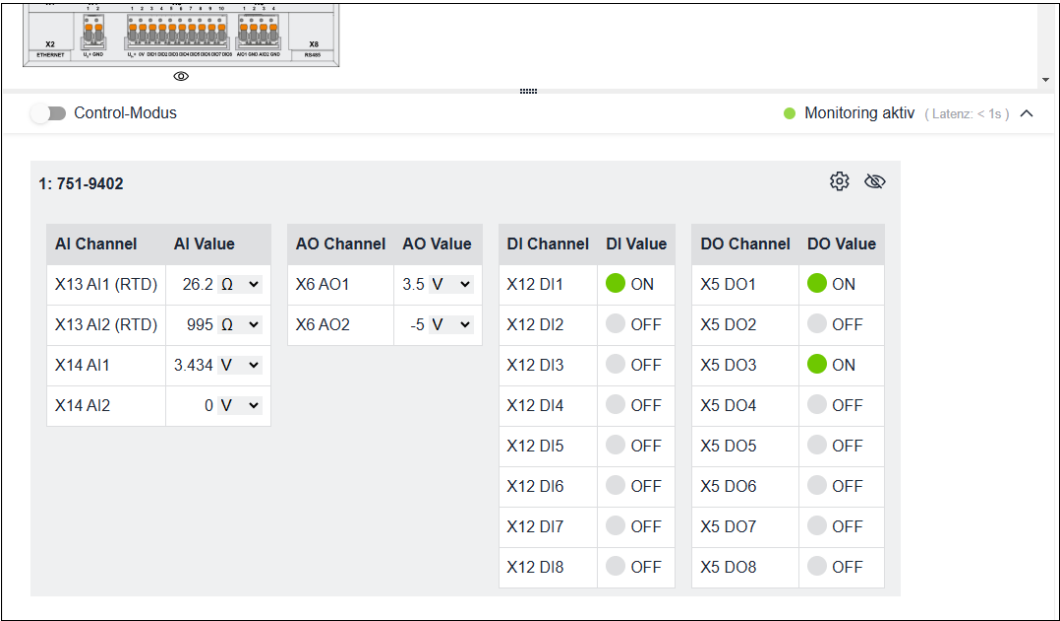


Abbildung 8: Monitormodus aktiv (Beispiel)

Darstellung/Einstellung von Statuswerten

Die Darstellung von Statuswerten kann über Auswahlfelder wie folgt dargestellt werden:

- als Rohwert oder
- als skaliertes Wert mit Einheit.

Skalierte Darstellungen sind lediglich auf der Benutzeroberfläche einstellbar, die Kommunikation selbst erfolgt nach wie vor über Rohwerte.

Digitalwerte lassen sich per Schiebeschalter einstellen:

- Schalterstellung  entspricht 1 bzw. true
- Schalterstellung  entspricht 0 bzw. false

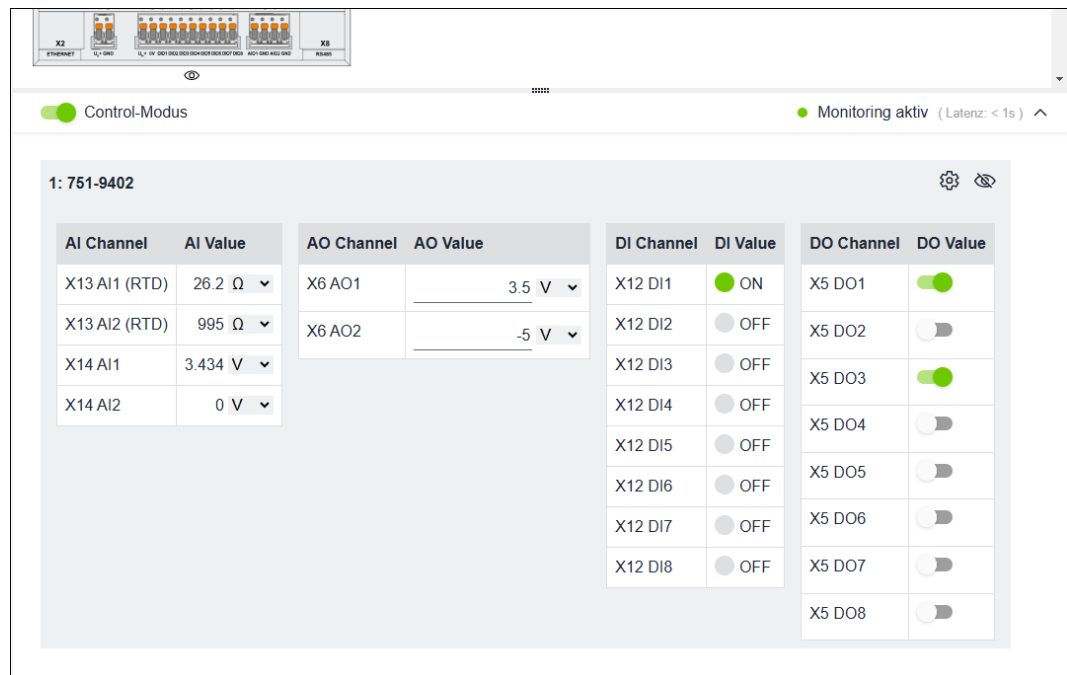


Abbildung 9: Control-Modus aktiv (Beispiel)

Hinweis

Ansicht „I/O-Check“ zeigt ggf. keine ursprüngliche Kanalkonfiguration

Bei Geräten, die eine variable Kanalkonfiguration unterstützen (z. B. der WAGO Compact Controller 100, Art.-Nr. 751-9402/xxx-xxx), kann die Zuordnung der Kanäle in der Ansicht „Einstellungen“ > „I/O-Channels“ geändert werden. In der Ansicht „I/O-Check“ werden dann nicht die ursprünglichen, sondern die geänderten Kanäle dargestellt.

Tipp:

Eine Übersicht der LED-Anzeigen/Statusmeldungen erreichen Sie auch über die Ansicht „Einstellungen“ > „LEDs“.

Außerdem verfügt jede Seite unter Einstellungen über einen Bereich „Gerätestatus/-aktionen“.

4.4.1.4.2 Einstellungen

In der Ansicht „Einstellungen“ werden die Parameter und Einstellungen des Gerätes als Zielwerte und aktuelle Werte gegenübergestellt. Parameter können in dieser Ansicht angepasst, auf das Gerät geschrieben oder vom Gerät gelesen werden.

Parameter und Einstellungen beziehen sich auf das verbundene Gerät (1).

Im oberen Bereich (2) wird angezeigt, ob aktuelle Gerätewerte und Projektwerte übereinstimmen. Die Gerätewerte können über die Schaltfläche **[Aktualisieren]** erneut ausgelesen werden.

Über die Register auf der linken Seite (8) werden Geräteparameter nach bestimmten Inhalten thematisch gebündelt, beispielsweise Einstellungen zum Netzwerk, zum Routing oder Cloud-Spezifika. Welche und wie viele Register angezeigt werden, ist gerätespezifisch unterschiedlich und resultiert aus der jeweiligen Gerätebeschreibungsdatei.

In den einzelnen Registern werden Einstellungen und Parameternamen gruppiert angezeigt (6). Es werden jeweils die Zielwerte (5) und die aktuellen Werte des Gerätes (3) dargestellt. Diese Werte werden miteinander abgeglichen und bei Abweichungen gekennzeichnet (4).

Zur Bearbeitung projektierter Werte werden unterschiedliche Steuerelemente (z. B. Textfelder, Auswahlfelder und Schieberegler) verwendet. In jedem Register werden wiederum Schaltflächen zum Schreiben in das Gerät oder zum Übernehmen als Zielwert angezeigt. Diese Schreib-/Leseoperationen gelten nur für die jeweils geöffnete Registerseite.

Verschiedene Onlineaktionen werden im unteren Bereich „Gerätestatus/-aktionen“ eines Registers angezeigt, sofern verfügbar (7). Einige Register beinhalten ausschließlich Onlineaktionen (z. B. „PasswordManagement“). Onlineaktionen werden immer sofort ausgeführt und sind unabhängig von der Lese-/Schreibfunktion. Sie werden direkt auf dem Gerät ausgeführt (Beispiel: Umstellen der Systemzeit). Es werden dabei keine Änderungen im Projekt vorgenommen.

1: Einstellungen von 751-9402

2: ✓ Einstellungen synchron vor 30 Minuten

3: Aktuelle Werte vor 30 Minuten

4: Vergleichssymbol (≠)

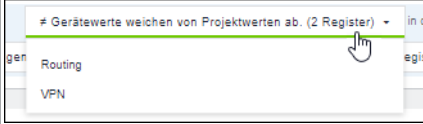
5: Zielwerte (Default-Werte setzen, Nur relevante anzeigen)

6: Einstellungen (Bridge Configuration, Port-Mapping, Bridge 1 (br0), Bridge 2 (br1), IP Configuration Sources, IP Configuration Addresses, IP Configuration Static Default Gateway, EthernetPort 1 (X1), EthernetPort 2 (X2), Enabled, Speed Duplex, MAC Learning, DNS, Custom DNS Servers)

7: Gerätestatus/-aktionen (vor einer Minute)

8: Systemkomponenten (I/O-Channels, Virtual Interfaces, Routing, NetworkNames, VPN, Serial Interface, AIDE, BACnet, CloudConnectiv..., CODESYS V3, Docker, FTP, FirmwareImage, MemoryCard, NTPClient, PasswordManag..., SNMP, SSH, LEDs, SystemRecovery)

Abbildung 10: Ansicht „Einstellungen“ (Beispiel)

Pos.	Parameter/Element	Beschreibung
1	Einstellungen von 751-9402	Artikelnummer des Gerätes Falls im Projekt ein Name für das Gerät vergeben wurde: Name (Artikelnummer) Auf dieses Gerät beziehen sich die nachfolgend dargestellten Einstellungen.
2	Status der Zielwerte/Gerätewerte und Anzeige, wie lange die letzte Synchronisation her ist:	
	✓ Einstellungen synchron	Die aktuellen Gerätewerte und Zielwerte stimmen überein.
	≠ Gerätewerte weichen von Zielwerten ab. (x Register)	Die aktuellen Gerätewerte weichen von den Zielwerten ab. Es wird angezeigt, in wie vielen Registern es Unterschiede gibt. Per Klick kann die Liste der Register angezeigt und direkt zu den Registern gewechselt werden. 
	vor __ Minuten/Stunden ↻	Es wird angezeigt, wie lange die letzte Synchronisation her ist. Über das Aktualisieren-Icon werden die Werte aller Register des Gerätes eingelesen und mit den Zielwerten abgeglichen.
3	Spalte „Aktuelle Werte“ vor __ Minuten/Stunden ↻	Zeigt die Werte eines Gerätes an. Die angezeigten Gerätewerte werden aktualisiert, wenn Zielwerte in das Gerät geschrieben werden oder wenn auf ein Aktualisieren-Icon geklickt wird. Das Aktualisieren-Icon neben „Aktuelle Werte“ gilt hier für das aktuell geöffnete Register. Im Header der Spalte wird außerdem angezeigt, wie lange die letzte Synchronisation der Gerätewerte her ist.
4	Vergleich zwischen „Zielwert“ und „Aktuellem Wert“ ≠	Zwischen den Spalten „Zielwerte“ und „Aktuelle Werte“ wird ein Ungleichzeichen angezeigt, sofern die Zielwerte und Gerätewerte voneinander abweichen. Das Ungleichzeichen wird als Markierung neben dem jeweiligen Registernamen übernommen, damit Abweichungen auch in ungeöffneten Registern schnell gefunden werden.
5	Spalte „Zielwerte“ - Defaultwerte setzen	Zeigt die Zielwerte für Einstellungen und Parameter an. „Defaultwerte setzen“ setzt die Zielwerte auf Standardwerte zurück. Die Werte können über das Auswahlfeld entweder nur für „Dieses Register“ oder für „Alle Register“ zurückgesetzt werden.
	Nur relevante anzeigen	☐ Zeigt alle Zielwerte und aktuellen Gerätewerte an (Standardeinstellung). Die in der aktuell gewählten Konfiguration irrelevanten Einstellungen und Parametergruppen werden ausgegraut/kursiv dargestellt. Sie sind nicht änderbar und werden nicht übertragen. Ein irrelevanter Parameter kann z. B. die Angabe einer festen IP-Adresse bei gleichzeitiger DHCP-Konfiguration sein. Die Auswertung, ob Zielwerte und Gerätewerte einander entsprechen, erfolgt lediglich auf Basis der relevanten Zielwerte. ☒ Zeigt nur die in der gewählten Konfiguration relevanten Ziel- und Gerätewerte an. Die Auswertung auf Relevanz erfolgt auf Basis der Zielwerte.
6	Gruppe/Parameter	Zeigt thematisch gruppiert Einstellungen und Parameter des Gerätes an, die aus der Gerätebeschreibung resultieren.
7	Bereich „Gerätestatus/-aktionen“ vor __ Minuten/Stunden ↻	In diesem Bereich wird der aktuelle Gerätestatus angezeigt. Geräteaktionen können direkt auf dem Gerät ausgeführt werden. Es werden dabei keine Änderungen in den Zielwerten vorgenommen.
8	Register	Die einzelnen Register fassen Einstellungen inhaltlich verwandter Themen zusammen. Registeranzahl und -inhalt sind gerätespezifisch.

Erläuterung von Icons und Bedienelementen der Ansicht „Einstellungen“

Tabelle 61: Icons und Bedienelementen der Ansicht „Einstellungen“

Icon	Beschreibung
	Ausrufezeichen-Icon Das Ausrufezeichen-Icon gibt Hinweise zur Validierung: - Ein Ausrufezeichen an einem Register bedeutet, dass dieses Register mindestens einen Parameter mit einer Warnung beinhaltet. - Ein Ausrufezeichen an einem Parameter bedeutet im Allgemeinen, dass der Parameter keinen passenden Wert bzw. kein passendes Format besitzt (z. B. Format einer IP-Adresse). Die Prüfung erfolgt als „Offline“-Validierung anhand der Gerätebeschreibung. Eine Warnung mit Ausrufezeichen ist nicht schreibverhindernd. - Ein Ausrufezeichen an einem Parameter, der in ein Gerät geschrieben wurde, bedeutet, dass der Parameter nicht vom Geräte akzeptiert wurde („Online“-Validierung). In diesem Fall wird das Ausrufezeichen rot angezeigt . Die Validierung von Werten findet also im Gerät selbst (online) statt. Die Offline-Validierung dient als einfache Art der Wertprüfung nach bestimmten Kriterien. Das Ausrufezeichen bleibt bis zur nächsten Änderung des Parameters bestehen.
beta	„Beta“-Markierung Die „Beta“-Markierung an einem Register kennzeichnet einen Stand an verfügbaren Einstellungen und Parametern, der sich für zukünftige Weiterentwicklungen (z. B. für neuere Firmwareversionen des Gerätes, Änderung der Oberfläche etc.) ändern kann.
	Aktualisieren-Icon Gerätewerte werden nicht automatisch vom Gerät abgefragt und angezeigt. Dies erfolgt einmalig bei einem Verbindungsaufbau und danach erst wieder durch Anklicken des Aktualisieren-Icons. Neben dem Icon wird angezeigt, wie lange die letzte Abfrage der Gerätewerte her ist.
	Sprechblasen-Icon Bei einem Klick auf ein Sprechblasen-Icon, werden Informationen/Hinweise zu bestimmten Parametern angezeigt. Bei einem Klick in einen anderen Bereich werden die Informationen wieder ausgeblendet.
	Tabellenansicht-Icon Listen mit diesem Icon können zur besseren Übersicht auch tabellarisch dargestellt werden. Bei einem Klick auf das Icon, wird die Tabelle in einem Dialogfenster geöffnet. Die Tabelle zeigt entweder die „Zielwerte“ oder die „Aktuellen Werte“ an. Die Umschaltung erfolgt über die entsprechende Toggle-Schaltfläche Projektwerte  Gerätewerte . Die Tabelle wird über folgende Schaltflächen bearbeitet:  Listenelement bearbeiten  Listenelement eine Position nach oben schieben  Listenelement eine Position nach unten schieben  Listenelement löschen  Neues Listenelement hinzufügen
	Ungleichzeichen Zwischen den Spalten „Zielwerte“ und „Aktuelle Werte“ wird ein Ungleichzeichen angezeigt, wenn die Zielwerte und aktuellen Gerätewerte voneinander abweichen. Das Ungleichzeichen wird als Markierung neben dem jeweiligen Registernamen übernommen, damit Abweichungen auch in ungeöffneten Registern schnell gefunden werden.

Datei-Handling

An verschiedenen Stellen in den Registern ist es möglich, Dateien hoch-/herunterzuladen. Außerdem ist es möglich, für Dateien bestimmte Aktionen zu speichern, die ausgeführt werden sollen, wenn eine Übertragung/Schreiben in das Gerät erfolgt.

Tabelle 62: Datei-Handling

Icon	Beschreibung
	Herunterladen der Datei auf den gewählten Speicherort.

Icon	Beschreibung
▼	Öffnet ein Auswahlmenü mit folgenden Optionen: Nicht gesetzt Beim Schreiben der Projektdaten in das Gerät wird keine Aktion ausgeführt. Die Datei auf dem Gerät (sofern vorhanden) bleibt unverändert. Auswählen Öffnet den Datei-Explorer zur Auswahl einer Datei. Der Inhalt der ausgewählten Datei wird beim Schreiben in das Gerät in die entsprechende, bereits vorhandene Datei auf dem Gerät übernommen. Datei auf Gerät bereinigen Der Inhalt der Datei auf dem Gerät (nicht die Datei selbst) wird beim Schreiben in das Gerät gelöscht.

4.4.1.4.3 Neustart

In dieser Ansicht wird der Verbindungsstatus des verwendeten Gerätes angezeigt. Durch Anklicken der Schaltfläche **[Gerät neu starten]** wird der Neustart des Gerätes initiiert.

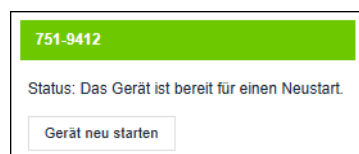


Abbildung 11: Ansicht „Neustart“

4.4.1.4.4 Firmware

In dieser Ansicht kann die Firmware des online verbundenen Gerätes aktualisiert werden.

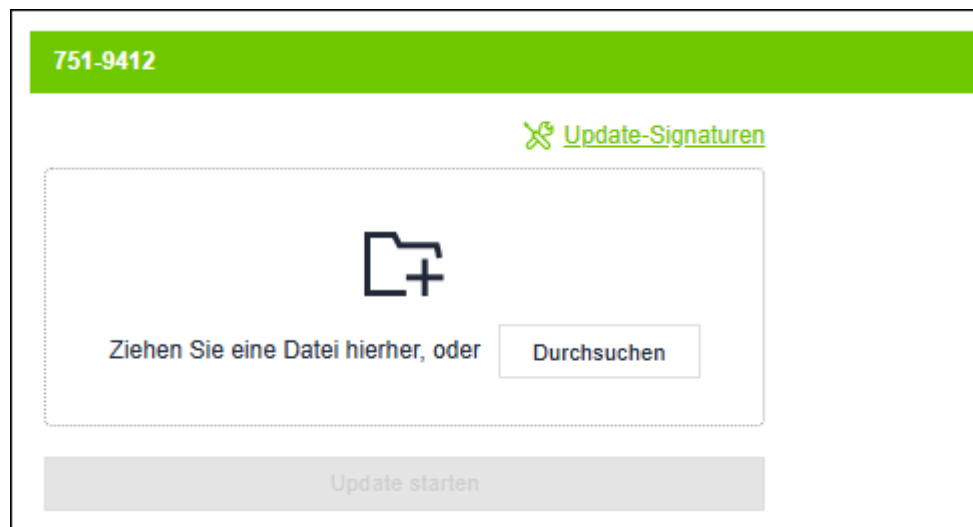


Abbildung 12: Ansicht „Firmware“

Option/Schaltfläche	Beschreibung
[Update Signaturen]	Öffnet das Register „Einstellungen“ und dort die Seite „UpdateSignatures“. Falls Firmware mit WAGO fremden und/oder mehreren Komponenten geladen wird, müssen auf der Seite „UpdateSignatures“ entsprechende Zertifikate hochladen werden, mit welchen die Signatur des gesamten Firmwareupdates geprüft werden kann.
📁 oder [Durchsuchen]	Auf den Ablagebereich kann per Drag and Drop eine Updatedatei gezogen werden. Alternativ ist die Datei über [Durchsuchen] in einem Dateibrowser auswählbar.
[Andere Datei auswählen]	Wird angezeigt, wenn bereits eine Updatedatei ausgewählt wurde. Über die Schaltfläche kann die Updatedatei noch einmal geändert werden.

Option/Schaltfläche	Beschreibung
[Update starten]	Führt das Firmwareupdate mit der ausgewählten Updatedatei durch.

4.4.1.4.5 Backup/Restore

Mit der **Backup-Funktion** können Gerätedaten gesichert werden. Als Ablageort für die Backup-Datei dient ein Netzwerk-/PC-Ordner oder ein am Gerät angestecktes Wechselmedium (SD-Karte oder USB-Speicher). Das Backup wird per Passworteingabe verschlüsselt abgelegt und beinhaltet Einstellungen, Nutzerdaten und die CODESYS Applikation.

Mit der **Restore-Funktion** können Gerätedaten aus einer Backup-Datei wiederhergestellt werden. Dazu muss das Passwort, welches bei der Erstellung des Backups verwendet wurde, erneut eingegeben werden.

i Hinweis

Firmwareversion beachten!

Das Wiederherstellen (Restore) ist nur möglich, wenn die Firmwareversionen zum Sicherungs- und Wiederherstellungszeitpunkt gleich sind.

i Hinweis

Backup/Restore kann mehrere Minuten dauern!

Das Erstellen der Backup-Dateien sowie das Wiederherstellen der Daten kann mehrere Minuten dauern.

Abbildung 13: Ansicht „Backup/Restore“

Option/Schaltfläche	Beschreibung
Ablageort	Auswahl des Ablageortes der Backup-Datei 🔄 Aktualisiert die Liste möglicher Ablageorte.

Option/Schaltfläche	Beschreibung
Passwort / Passwort wiederholen	Eingabefeld für das Passwort, mit welchem die Backup-Datei gesichert werden soll. Die Eingabe eines Passwortes ist Voraussetzung für das Starten des Backups. ❗ Passworteingabe fehlt. 🔍 Passwort in Klartext anzeigen.
[Backup-Vorgang starten]	Die Schaltfläche wird freigegeben, sobald ein Passwort für das Backup eingegeben wurde und andere Prozesse (z. B. Restore oder Firmwareupdate) abgeschlossen sind. Nach dem Erstellen der Backup-Datei, wird sie zunächst als Archivdatei (*.zip) in den „Downloads“-Ordner heruntergeladen.
Backup-Quelle	Auswahl des Ablageortes der Backup-Quelle 🔄 Aktualisiert die Liste der Ablageorte für die Backup-Quellen.
Passwort	Eingabefeld für das Passwort, mit welchem die Backup-Datei gesichert wurde. Die Prüfung des Passwortes erfolgt im folgenden Restore-Prozess vom Gerät selbst. ❗ Passworteingabe fehlt. 🔍 Passwort in Klartext anzeigen.
🔍 oder [Durchsuchen]	Der Ablagebereich 🔍 wird angezeigt, sofern als Backup-Quelle das Dateisystem ausgewählt wurde. Auf den Ablagebereich kann per Drag and Drop eine Backup-Datei zur Wiederherstellung gezogen werden. Alternativ ist die Backup-Datei über [Durchsuchen] in einem Dateibrowser auswählbar.
[Restore-Vorgang starten]	Die Schaltfläche wird freigegeben, sobald das Passwort eingegeben wurde und eine gültige Backup-Datei ausgewählt wurde. [Restore-Vorgang starten] startet den Wiederherstellungsprozess.

4.4.1.4.6 Geräte-Log

In dieser Ansicht können protokollierte Log-Einträge des Gerätes angezeigt werden.

Über Anzeigefilter können vor dem Abrufen der Log-Einträge verschiedene Log-Level (Schweregrad der Meldung) zur Ansicht gewählt werden.

Die Sortierung der Einträge erfolgt nach Zeitstempel. Der neueste Eintrag befindet sich am unteren Ende der Liste.

❗ Hinweis

Geräte-Log im Register „Einstellungen“ konfigurieren!

Welche Gerätemeldungen generell geloggt werden, konfigurieren Sie im Register „Einstellungen“ unter „Logging“. Das Register „Geräte-Log“ dient lediglich als Anzeige der konfigurierten Geräte-Logs und bietet zusätzliche Filtermöglichkeiten.

751-9412

Max. Anzahl Einträge	100	Min. Log-Level	Informational ▼
Log-Quellen	Zum Beispiel: kernel oder sppd.service	Log-Einträge (ab Zeitpunkt)	☐ 27.06.25, 06:57 7
Datei-Ausgabeformat	TXT ▼		

Log-Einträge abrufen

Log-Einträge als Datei abrufen

Anzahl Log-Einträge: 100

Fri Jun 06 2025 14:37:00 GMT+0200 (Mitteleuropäische Sommerzeit) # wcs-rollout.service [354] # Informational(6) Reconfig Trigger: Firewall - Apply ruleset
Fri Jun 06 2025 14:37:00 GMT+0200 (Mitteleuropäische Sommerzeit) # wcs-rollout.service [354] # Informational(6) Reconfig Trigger: Firewall - IP filter
Fri Jun 06 2025 14:37:00 GMT+0200 (Mitteleuropäische Sommerzeit) # wcs-rollout.service [354] # Informational(6) Reconfig Trigger: HostnameDisableDHCP
Fri Jun 06 2025 14:37:00 GMT+0200 (Mitteleuropäische Sommerzeit) # wcs-rollout.service [354] # Informational(6) Reconfig Trigger: PasswordQuality
Fri Jun 06 2025 14:37:00 GMT+0200 (Mitteleuropäische Sommerzeit) # wcs-rollout.service [354] # Informational(6) Reconfig Trigger: Device Certificate AutoRenewal

Abbildung 14: Register „Geräte-Log“

Option/Schaltfläche	Beschreibung
Max. Anzahl Einträge	Legt die maximale Anzahl der Einträge fest, die vom Gerät gelesen werden (standardmäßig 100). In diesem Register können maximal 1.000 Log-Einträge abgerufen und angezeigt werden. Beim Speichern in eine Datei lässt sich die Anzahl auf 100.000.000 Einträge erhöhen.
Min. Log-Level	Filtert die angezeigten Log-Einträge nach dem Log-Level.
Log-Quellen	Filtert die Log-Quellen der Log-Einträge nach der eingegebenen Zeichenkette und zeigt nur entsprechend passende Einträge an.
Log-Einträge (ab Zeitpunkt)	Bei Auswahl dieser Option können über einen Kalender das Datum und die Uhrzeit ausgewählt werden, ab welchem die Log-Einträge angezeigt werden. Auf diese Weise können die Ergebnisse beispielsweise auf die letzten 20 Minuten eingeschränkt werden.
Datei-Ausgabeformat	Sofern „Log-Einträge als Datei abrufen“ ausgewählt wird: Wählt das Ausgabeformat für die Datei, in der Log-Einträge gespeichert werden. Zur Verfügung stehen das Textformat „TXT“ oder das Tabellenformat „CSV“.
[Log-Einträge abrufen]	Zeigt die Log-Einträge basierend auf der Konfiguration und entsprechend der gewählten Filter an.
[Log-Einträge als Datei abrufen]	Öffnet einen Dateieexplorer zum Speichern der Log-Einträge basierend auf der Konfiguration und entsprechend der gewählten Filter.
Inhalt der Tabelle	Zeigt für jeden Log-Eintrag folgende Informationen an: Zeitstempel (Erstellungszeitpunkt des Eintrages), Quelle (Service/Dienst, welcher den Log-Eintrag erstellt hat), Log-Level (Schweregrad des Eintrages) sowie ggf. weitere Informationen, abhängig von Quelle/Dienst Die Sortierung der Einträge erfolgt nach Zeitstempel von alt (oben) nach neu (unten).

4.4.1.5 Meldungsfenster

Die Meldungsleiste bzw. das Meldungsfenster befindet sich im unteren Bereich der Oberfläche. Hier werden während der Konfiguration kontinuierlich Fehler, Warnungen, Erfolgsmeldungen und zusätzliche Informationen angezeigt.

Zunächst wird die Meldungsleiste angezeigt:

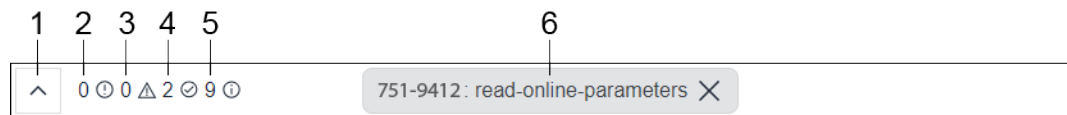


Abbildung 15: Meldungsleiste

Pos.	Beschreibung
1	Öffnet das Meldungs Fenster für detaillierte Informationen. Minimiert das Meldungs Fenster und zeigt die Meldungsleiste an.
2	Zeigt die Anzahl der Fehler an. Die Anzeige blinkt, bis das Meldungs Fenster geöffnet wird.
3	Zeigt die Anzahl der Warnungen an.
4	Zeigt die Anzahl der Erfolgsmeldungen an.
5	Zeigt die Anzahl zusätzlicher Informationen an.
6	Zeigt für einige Sekunden die letzte Meldung an. Bei Fehlermeldung wird die Meldung rot hinterlegt.

Die vollständige Liste der Meldungen mit detaillierten Informationen wird im Meldungs Fenster angezeigt. Dieses wird über die Schaltfläche der Meldungsleiste geöffnet:

▼	🔴 1 Fehler	🟡 0 Warnungen	🟢 1 Erfolge	📘 6 Infos	🗑️ Löschen	🔄 Wiederherstellen	💾 Speichern	📌 Pin	🔍
Beschreibung	Quelle	Meldungszeit							
📘 Gerätewerte lesen: abgeschlossen	Einstellungen	2026-03-03 10:44:04							
📘 > Gerätewerte lesen: in Bearbeitung	Einstellungen	2026-03-03 10:44:04							
📘 > Gerätewerte lesen: in Bearbeitung	Einstellungen	2026-03-03 10:44:03							
🔴 Fehler beim Aktualisieren des Lizenz-Repositorys (im Lizenz-Client)	Lizenzen	2026-03-03 10:44:03							
📘 Gerätewerte lesen: gestartet	Einstellungen	2026-03-03 10:44:00							
🟢 Verbunden mit 192.168.1.43	WDA-Verbindung	2026-03-03 10:44:00							
📘 Versuche Verbindung aufzubauen zu 192.168.1.43	WDA-Verbindung	2026-03-03 10:43:57							
📘 > Neues Gerät zum Projekt hinzugefügt	Projekt	2026-03-03 10:43:57							

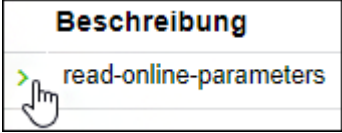
Abbildung 16: Meldungs Fenster

Standardmäßig werden beim Öffnen des Meldungs Fensters alle Meldungen angezeigt.

Über die Schaltflächen „Fehler“, „Warnungen“, „Erfolge“ und „Infos“ können die Meldungen gefiltert werden. Bei aktiviertem Zustand (Schaltfläche farbig dargestellt) werden nur die gefilterten Meldungen in der Liste angezeigt. Nach nochmaligem Anklicken (Schaltfläche weiß dargestellt) werden die Meldungen wieder ausgeblendet.

Folgende Funktionen können über die Schaltflächen ausgeführt werden:

Schaltfläche / Tabelleneintrag	Beschreibung
🔴 1 Fehler	Zeigt Fehler bei der Konfiguration an.
🟡 0 Warnungen	Zeigt Warnungen bei der Konfiguration an.
🟢 1 Erfolge	Zeigt Erfolgsmeldungen an (z. B. erfolgreich verbundene Geräte oder erfolgreich übertragene Daten).
📘 6 Infos	Zeigt Statusmeldungen/Informationen zur Konfiguration an.
🗑️ Löschen	Entfernt die angezeigten Meldungen aus der Liste.
🔄 Wiederherstellen	Stellt entfernte Meldungen wieder her.
💾 Speichern	Öffnet ein Dialogfenster zum Speichern aller angezeigten Meldungen als Textdatei. Je nach PC-Konfiguration erfolgt der Download ggf. direkt in den Downloads-Ordner.
📌 Pin	Hält das Fenster sichtbar und ausgeklappt im Vordergrund.

Schaltfläche / Tabelleneintrag	Beschreibung
 Unpin	Löst das angepinnte Meldungsfenster. Wird nach dem Lösen in einen anderen Seitenbereich geklickt, wird das Fenster zu einer Meldungsleiste minimiert.
	Sucht und filtert nach beliebigen Texten im Meldungsfenster. Die Eingabe eines Zeichens aktiviert die Suchfunktion für die Spalten „Gerät“, „Beschreibung“ und „Quelle“ und stellt gefundene Treffer grün hinterlegt dar. Zeilen ohne Treffer werden ausgeblendet.
Beschreibung	Zeigt die Beschreibung der Meldung an. Für umfangreichere Meldungen können per Schaltfläche weitere Informationen geöffnet werden. 
Quelle	Zeigt die Quelle der Meldungen an, beispielsweise „Einstellungen“.
Meldungszeit	Zeigt Datum und Uhrzeit der Erstellung der Meldung an. Dabei steht die neueste Meldung oben.

4.5 Netzwerkfunktionen

4.5.1 Netzwerkkonfiguration

4.5.1.1 Konfiguration für SECURITY-Anforderungen

Um den Controller sicher im Netzwerk zu betreiben, müssen die folgenden Konfigurationsparameter entsprechend der Netzwerk-Infrastruktur eingestellt werden:

- Alle nicht genutzten ETHERNET-Ports müssen abgeschaltet werden (Enable = FALSE).
Damit ist ein Zugriff von außen nicht mehr möglich.
- Netzwerksegmentierung per Bridgekonfiguration
 - Gemeinsame Bridge mit mehreren Ethernetports --> Switching von Netzwerkpaketen
 - Nur ein ETHERNET-Port je Bridge --> kein Switching der Netzwerkpakete
- IP-Adressierung
 - Statisch
 - Automatisch per DHCP-Bezug
- Defaultgateway
 - Per Konfiguration
 - Automatisch per DHCP-Bezug
- Host- und Domainname
 - Per Konfiguration
 - Automatisch per DHCP-Bezug
- DNS-Server
 - Per Konfiguration
 - Automatisch per DHCP-Bezug

In der Werkseinstellung ist der automatische Bezug über DHCP eingestellt. Damit werden die folgenden Werte automatisch im System konfiguriert:

- Das Defaultgateway
- Der Hostname

Da das DHCP-Protokoll auf Broadcast basiert, muss das Netzwerk entsprechend abgesichert werden.

4.5.1.2 Schnittstellenkonfiguration

4.5.1.2.1 Bridge-und Portkonfiguration

Bei Nutzung von gemeinsamen Ports (Switched Mode) sind beide physikalischen Netzwerkports Teil desselben Netzwerks.

Weitergeleitete Pakete werden auf Layer 2 Ebene nicht gefiltert.

Tabelle 63: „Einstellungen“ – „Bridge Configuration“

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

Tabelle 64: „Einstellungen“ – „Bridge 1 ... Bridge <n>“

Parameter	Bedeutung	
Bridge <n>	Für jede im Controller vorhandene Bridge wird ein eigenes Register angezeigt.	
Adresses	Eingabe der IP-Adressen für die ausgewählte Bridge als kommaseparierte Liste im CIDR-Format	
Gateway	Eingabe der Gateway-Adresse	
Gateway Metric	Eingabe der Gateway-Metric; Werkseinstellung: „200“	
Sources	Auswahl, ob per DHCP übertragene IP-Adressen verwendet werden	
	DHCP	Es werden per DHCP übertragene IP-Adressen und die unter „Adresses“ eingegebenen IP-Adressen verwendet.
	„Leer“	Es werden nur die unter „Adresses“ eingegebene IP-Adressen verwendet.
DHCP - RouteMetric	Eingabe der Metrik für per DHCP übertragene Routen; Werkseinstellung: „100“ Dieses Eingabefeld ist nur aktiv, wenn im Auswahlfeld „Sources“ der Wert „DHCP“ eingestellt ist.	
DHCP - UseDNS	Einstellung, ob per DHCP übertragene DNS-Adressen verwendet werden. Dieses Kontrollfeld ist nur aktiv, wenn im Auswahlfeld „Sources“ der Wert „DHCP“ eingestellt ist.	
DHCP - UseDomains	Auswahl, ob und wie per DHCP übertragene Domains verwendet werden; Dieses Auswahlfeld ist nur aktiv, wenn im Auswahlfeld „Sources“ der Wert „DHCP“ eingestellt ist.	
	False	Per DHCP übertragene Domains werden nicht verwendet.
	True	Per DHCP übertragene Domains werden als Search-Domain verwendet.
	Route	Per DHCP übertragene Domains werden als Routing-only-Domains verwendet.
DNS	Eingabe der IP-Adressen der DNS-Server als kommaseparierte Liste	
Domains	Eingabe der Domainadressen als kommaseparierte Liste; Wenn einer Adresse eine Tilde (~) vorangestellt wird, wird die Domain als Routing-only-Domain verwendet. Wenn einer Adresse keine Tilde (~) vorangestellt wird, wird die Domain als Search-Domain verwendet.	
MTU	Eingabe des MTU-Wertes; Werkseinstellung: „1500“	

Um den Controller vor Prozessorlastüberlast zu schützen, kann die Stormprotection-Funktion für den zu erwartenden Netzwerkverkehr (bzgl. Broad- und Multicast-Raten) konfiguriert werden:

- Die Stormprotection-Rate wird global für alle ETHERNET-Ports eingestellt
- Für alle ETHERNET-Ports kann global eingestellt werden, ob die eingestellte Broadcast-Rate auch für Multicast gelten soll.
- Die Stormprotection-Funktion kann für jeden ETHERNET-Port getrennt aktiviert werden.

Tabelle 65: „Einstellungen“ – „Networking/StormProtection“

Parameter	Bedeutung
Broadcast Rate Limit	Broadcast Rate Limit einstellen. Werkseinstellung: „10 %“
Multicast Rate Limit	Dieses Eingabefeld ist nicht aktiv. Es ist nicht sichtbar, wenn das Kontrollfeld „Nur relevante anzeigen“ oben auf der Seite aktiviert ist.
Enable Multicast Rate Limiting	Multicast Rate Limiting aktivieren/deaktivieren.
	☐ Multicast Rate Limiting ist deaktiviert. Der eingestellte Broadcast-Rate-Grenzwert wird nur auf Broadcast-Nachrichten angewendet. (Werkseinstellung)
	☒ Multicast Rate Limiting ist aktiviert. Der eingestellte Broadcast-Rate-Grenzwert wird auf Broadcast- und Multicast-Nachrichten gemeinsam angewendet.

Tabelle 66: „Einstellungen“ – „EthernetPort 1 ... EthernetPort <n>“

Parameter	Bedeutung
EthernetPort <n> (X<n>)	Für jeden im Controller vorhandenen Port wird ein eigenes Register angezeigt.
Enabled	Ausgewählten Port aktivieren/deaktivieren.
	☐ Der Port ist deaktiviert.
	☒ Der Port ist aktiviert.
Speed Duplex	Übertragungsgeschwindigkeit und Übertragungsverfahren auswählen. Das Auswahlfeld ist nur aktiv, wenn der Port aktiviert ist. Mit der Auswahl „Autonegotiation“ werden die Verbindungsmodalitäten automatisch mit der Gegenstelle ausgehandelt. Werkseinstellung: „Autonegotiation“
MAC Learning	„MAC Learning“-Funktionalität für den ausgewählten Port aktivieren/deaktivieren. Das Kontrollfeld ist nur aktiv, wenn der Port aktiviert ist.
	☐ Die „MAC Learning“-Funktionalität ist deaktiviert.
	☒ Die „MAC Learning“-Funktionalität ist aktiviert.
Enable Broadcast Rate Limiting	Broadcast Protection für den ausgewählten Port aktivieren/deaktivieren.
	☐ Broadcast Protection ist deaktiviert.
	☒ Broadcast Protection ist aktiviert.
Enable Multicast Rate Limiting	Dieses Kontrollfeld ist nicht aktiv. Es ist nicht sichtbar, wenn das Kontrollfeld „Nur relevante anzeigen“ oben auf der Seite aktiviert ist.

Für jede Bridge wird im Bereich „Gerätestatus/-aktionen“ eine eigene Gruppe angezeigt.

Tabelle 67: „Gerätestatus/-aktionen“ – „Bridge <n> (br<n-1>)“

Parameter	Bedeutung
MAC Address	MAC-Adresse der ausgewählten Bridge
Addresses	Anzeige der IP-Adressen als kommasseparierte Liste im CIDR-Format
Gateway	Anzeige der Gateway-Adresse
DNS	Anzeige der IP-Adressen der DNS-Server als kommasseparierte Liste
Domains	Anzeige der Domainadressen als kommasseparierte Liste; Wenn einer Adresse eine Tilde (~) vorangestellt wird, wird die Domain als Routing-only-Domain verwendet. Wenn einer Adresse keine Tilde (~) vorangestellt wird, wird die Domain als Search-Domain verwendet.

Für jeden ETHERNET-Port wird im Bereich „Gerätestatus/-aktionen“ eine eigene Gruppe angezeigt.

Tabelle 68: „Gerätestatus/-aktionen“ – „EthernetPort <n> (X<n>)“

Parameter	Bedeutung	
MAC Address	MAC-Adresse der ausgewählten ETHERNET-Schnittstelle	
Has Link	Anzeige des Verbindungsstatus	
	false	Die Schnittstelle ist nicht verbunden.
	true	Die Schnittstelle ist verbunden.
Speed Duplex	Anzeige der Übertragungsgeschwindigkeit und des Übertragungsverfahrens	

4.5.1.3 Hostname/Domainadressen

Der Hostname wird für den Controller global eingestellt.

Die Domainadressen werden für jede im Controller konfigurierte Bridge getrennt eingestellt.

4.5.1.3.1 Hostname

Ohne die Konfiguration eines Hostnamens bekommt der Controller einen Standardnamen. Dieser Name enthält einen Teil der Produktbezeichnung und die letzten drei Werte der MAC-Adresse des Controllers. Der Standardname gilt, solange noch kein Hostname konfiguriert wurde bzw. kein Hostname per DHCP an den Controller geliefert wurde.

Bei mehreren Netzwerk-Schnittstellen mit DHCP wird der Hostname übernommen, welcher zuletzt über DHCP übermittelt wird.

Der Standardhostname wird wieder aktiv, wenn die Netzwerk-Schnittstellen auf statische IP-Adressen umgestellt werden oder wenn die Leasetime des DHCP-Lease ausgelaufen ist.

Wenn der Hostname manuell konfiguriert wird, hat der konfigurierte Name die höchste Priorität und wird nicht durch über DHCP empfangenen Hostnamen überschrieben.

Die Einstellungen zum Hostnamen sind z. B. auf der WBM-Seite „Hostname“ in der Gruppe „Hostname“ möglich.

4.5.1.3.2 Domainadressen

Domainadressen können manuell in einer Liste eingetragen werden. Weiterhin ist eine automatische Übertragung per DHCP möglich, wenn der Controller entsprechend konfiguriert ist.

Sowohl bei den manuell eingetragenen Adressen als auch bei den per DHCP übertragenen Adressen kann vorgegeben werden, ob es sich bei den Domains um Search-Domains oder um Routing-only-Domains handelt.

Bei Search-Domains dient die Adresse als Suchsuffix, um Single-Label-Hostnamen auf vollqualifizierte Domännennamen (FQDNs) zu erweitern.

Bei Routing-only-Domains wird der gesamte DNS-Datenverkehr, der nicht mit einer anderen Domäne übereinstimmt, an diese Schnittstelle mit dem angegebenen DNS-Server weitergeleitet. Mit dieser Einstellung können Sie bestimmte DNS-Server bevorzugen.

Weitere Informationen zur Bedeutung und Konfiguration der Domainadressen finden Sie in der Dokumentation zu „systemd-networkd“ im Internet.

Die Einstellungen zu den Domainadressen sind z. B. im WBM oder im WAGO Device Manager unter „Einstellungen“ auf der WBM-Seite „Network“ in den Gruppen „Bridge 1 ... Bridge <n>“ möglich.

4.5.2 Netzwerksicherheit

4.5.2.1 Bereitstellen einer sicheren Netzwerkumgebung

Die Kommunikation über Standard-Feldbusprotokolle ist unsicher und es gibt keine Protokollmechanismen zur Absicherung.

Um Security-Anforderungen zu erfüllen, muss der Betreiber eine physikalische Absicherung vornehmen (z. B. geschützte Verlegung der Leitungen, Schutz vor unbefugtem Zutritt) oder der Zugang über VPN erfolgen.

4.5.2.2 Firewall

Die Firewall schützt den Controller vor unerwünschten Netzwerkzugriffen und startet bereits, bevor das Netzwerk aktiv wird.

Die Firewall muss entsprechend den betrieblichen Security-Anforderungen eingestellt werden.

Einstellbar sind:

- Zugelassene/gesperrte MAC- bzw. IP-Adressen
- Flood- und Broadcastschutz
- Freischaltung der Ports/Bridges für die verschiedenen Dienste

Die Einstellung kann über das WBM oder den WAGO Device Manager erfolgen.

Die Firewall ist auch während einer Umkonfiguration der Firewall-Parameter aktiv.

Zur Prüfung der Firewall können Zugriffsversuche mit in den Einstellungen nicht zugelassenen Ports oder Adressen durchgeführt werden. Diese Zugriffsversuche müssen abgewiesen werden.

4.5.2.2.1 MAC-Adressenfilter

Es können verschiedene Filterregeln für Absender-MAC-Adressen angelegt werden.

Für jede Filterregel sind folgende Einstellungen möglich:

- Name der Regel
- Aktivierung/Deaktivierung der Regel (Enabled/Disabled)
- Wirkung der Regel (Drop/Accept)

- Absender-MAC-Adresse
- Maske

Die Einstellung ist über das WBM oder über den WAGO Device Manager möglich.

Tabelle 69: „Einstellungen“ – „FirewallMACFilterRule Liste“

Parameter	Bedeutung	
FirewallMACFilterRule <n>	Für jede Filterregel wird eine eigene Gruppe angezeigt.	
Name	Eingabe des Namens für die Filterregel	
Enabled	Aktivierung/Deaktivierung der Filterregel	
	☐	Die Filterregel wird nicht angewendet.
	☒	Die Filterregel wird angewendet.
Verdict	Einstellung der Wirkung der Filterregel	
	Drop	Pakete mit der gefilterten Absender-MAC-Adresse werden verworfen.
	Accept	Pakete mit der gefilterten Absender-MAC-Adresse werden akzeptiert.
Address	Eingabe der von der Filterregel betroffenen Absender-MAC-Adresse	
Mask	Eingabe der Maske im Format „ff:ff:ff:ff:ff:ff“	

4.5.2.2.2 ServiceRules

Für jeden Dienst kann eine eigene FirewallServiceRule konfiguriert werden.

Für jede FirewallServiceRule können die zugeordneten Interfaces (Bridge) ausgewählt werden.

Die Liste der möglichen Interfaces wird aus den Einstellungen im Abschnitt „Bridge-und Portkonfiguration“ generiert.

- FirewallServiceRule <m>
 - Interfaces

Die Einstellung ist über das WBM oder über den WAGO Device Manager möglich.

4.5.2.2.3 IP-Adressenfilter

Es können verschiedene Filterregeln für Quell-IP-Adressen angelegt werden.

Für jede Filterregel sind folgende Einstellungen möglich:

- Name der Regel
- Aktivierung/Deaktivierung der Regel (Enabled/Disabled)
- Wirkung der Regel (Drop/Accept)
- Protokoll (TCP, UDP oder beide)
- Interfaces
- Quell-IP-Adresse (CIDR-Format)
- Quell-Port
- Ziel-Port

Die Einstellung ist über das WBM oder über den WAGO Device Manager möglich.

Tabelle 70: „Einstellungen“ – „FirewallIPFilterIncomingRule Liste“

Parameter	Bedeutung
FirewallIPFilterIncomingRule <n>	Für jede Filterregel wird eine eigene Gruppe angezeigt.
Name	Eingabe des Namens für die Filterregel
Enabled	Aktivierung/Deaktivierung der Filterregel

Parameter	Bedeutung	
	☐	Die Filterregel wird nicht angewendet.
	☒	Die Filterregel wird angewendet.
Verdict	Einstellung der Wirkung der Filterregel	
	Drop	Pakete mit der gefilterten Quell-IP-Adresse werden verworfen.
	Accept	Pakete mit der gefilterten Quell-IP-Adresse werden akzeptiert.
Protocol	Auswahl der IP-Protokolle	
	Any	„Any“ schließt auch „TCP“ und „UDP“ ein.
	TCP	
	UDP	
Interfaces	Auswahl der Interfaces, auf die die Regel angewendet wird: Wenn kein Interface ausgewählt ist, wird die Regel auf alle Interfaces angewendet.	
Source IP	Eingabe der Quell-IP-Adresse und -Maske im CIDR-Format	
Source Port	Eingabe des Quellports („0“ = alle)	
Destination Port	Eingabe des Zielports („0“ = alle)	

4.5.2.2.4 IP-Forwarding-Filter

Es können verschiedene Filterregeln für Quell- und Ziel-IP-Adressen angelegt werden. Für jede Filterregel sind folgende Einstellungen möglich:

- Name der Regel
- Aktivierung/Deaktivierung der Regel (Enabled/Disabled)
- Wirkung der Regel (Drop/Accept)
- Protokoll (TCP, UDP oder beide)
- Eingangs- und Ausgangs-Interfaces
- Quell-IP-Adresse (CIDR-Format)
- Quell-Port
- Ziel-IP-Adresse (CIDR-Format)
- Ziel-Port

Die Einstellung ist über das WBM oder über den WAGO Device Manager möglich.

Tabelle 71: „Einstellungen“ – „FirewallIPFilterForwardingRule Liste“

Parameter	Bedeutung	
FirewallIPFilterForwardingRule <n>	Für jede Filterregel wird eine eigene Gruppe angezeigt.	
Name	Eingabe des Namens für die Filterregel	
Enabled	Aktivierung/Deaktivierung der Filterregel	
	☐	Die Filterregel wird nicht angewendet.
	☒	Die Filterregel wird angewendet.
Verdict	Einstellung der Wirkung der Filterregel	
	Drop	Pakete werden gemäß Filterkriterien verworfen.
	Accept	Pakete werden gemäß Filterkriterien akzeptiert.
Protocol	Auswahl der IP-Protokolle	
	Any	„Any“ schließt auch „TCP“ und „UDP“ ein.
	TCP	

Parameter	Bedeutung
	UDP
Incoming Interfaces	Auswahl der Eingangs-Interfaces, auf die die Regel angewendet wird: Wenn kein Interface ausgewählt ist, wird die Regel auf alle Interfaces angewendet.
Outgoing Interfaces	Auswahl der Ausgangs-Interfaces, auf die die Regel angewendet wird: Wenn kein Interface ausgewählt ist, wird die Regel auf alle Interfaces angewendet.
Source IP	Eingabe der Quell-IP-Adresse und -Maske im CIDR-Format
Source Port	Eingabe des Quellports („0“ = alle)
Destination IP	Eingabe der Ziel-IP-Adresse und -Maske im CIDR-Format
Destination Port	Eingabe des Zielpports („0“ = alle)

4.5.2.2.5 Flood/Broadcast Protection

4.5.2.2.5.1 ICMP Echo Flood Protection

Die Firewall reduziert die Anzahl von ICMP-Echo-Paketen, so dass der Normalbetrieb nicht negativ beeinflusst wird, aber Angriffe unterbunden werden.

Die Anzahl von ICMP-Echo-Paketen ist auf maximal 10 Pakete pro Sekunde eingestellt, um mehrere parallele Pings nicht zu stören.

Die Einstellung kann nicht verändert werden.

4.5.2.2.5.2 ICMP Echo Broadcast Protection

Die Firewall verwirft Broadcast-Ping-Pakete.

Die Einstellung kann nicht verändert werden.

4.5.2.3 IPsec

Zur Absicherung über IPsec können verschiedene IKE-Verbindungen konfiguriert werden.

Für jede IKE-Verbindung sind folgende Einstellungen möglich:

- Name
- Authentifizierungsmethode („X.509“/„PSK“)
- Remote-Adresse
- Secret
- Lokales Zertifikat
- Lokale Identität
- Remote-CA-Zertifikat
- Remote-Zertifikat
- Remote-Identität

Für die Authentifizierungsmethode wird die Einstellung „X.509“ empfohlen.

Die Authentifizierung über PreSharedKeys („PSK“) ist unsicherer als die zertifikatsbasierte Authentifizierung mit Truststore („X.509“).

Für die Konfiguration der Remote-CA wird dringend empfohlen, eine IKE-Identität einzutragen.

Ohne die Konfiguration einer Identität wird jedes von der CA ausgestellte Zertifikat akzeptiert.

Es werden alle vom BSI als sicher eingestufteten IKE- und ESP-Algorithmen erlaubt. Diese Voreinstellung ist nicht konfigurierbar.

Die Konfiguration der IKE-Verbindungen kann im WBM oder im WAGO Device Manager auf der Seite „IPsecClient“ unter „Einstellungen“ durchgeführt werden.

Tabelle 72: „Einstellungen“ – „IKEConnection“

Parameter	Bedeutung
IKEConnection Liste	Anzahl der angelegten IKE-Verbindungen
IKEConnection <n>	Für jede angelegte IKE-Verbindung wird ein eigener Bereich angezeigt.
Name	Namen für die IKE-Verbindung eingeben.
Authentication Method	Authentifizierungsmethode der IKE-Verbindung auswählen; X.509 (empfohlen) PSK
Remote Address	Hostname oder IP-Adresse des IPsec-Responders eingeben.
Secret	„Pre-shared Key“ eingeben, der für die Authentifizierung verwendet wird, wenn die Authentifikationsmethode 'PSK' ausgewählt ist.
Local Certificate	Zertifikat des lokalen Peers eingeben
Local Identity	IKE-Identität des lokalen Peers eingeben. Wenn keine Identität konfiguriert ist, wird die Identität vom IPsec-Client automatisch bestimmt.
Remote CA Certificate	CA-Zertifikat auswählen, mit dem das Zertifikat der Gegenstelle signiert sein muss.
Remote Certificate	Zertifikat der Gegenstelle auswählen.
Remote Identity	IKE-Identität der Gegenstelle eingeben. Wenn keine Identität konfiguriert ist, wird jede Identität akzeptiert.

Zu jeder IKE-Verbindung können verschiedene IPsec-Tunnel konfiguriert werden.

Für jeden IPsec-Tunnel sind folgende Einstellungen möglich:

- Status (Enabled/Disabled)
- Quelladresse im CIDR-Format
- Zieladresse im CIDR-Format

Die Konfiguration der IPsec-Tunnel kann im WBM oder im WAGO Device Manager auf der Seite „IPsecClient“ unter „Einstellungen“ durchgeführt werden.

Tabelle 73: „Einstellungen“ – „IPsecTunnel“

Parameter	Bedeutung
IPsecTunnel Liste	Anzahl der angelegten IPsec-Tunnel
IPsecTunnel <n>	Für jeden angelegten IPsec-Tunnel wird ein eigener Bereich angezeigt.
Connection	IKE-Verbindung auswählen, für die der IPsec-Tunnel konfiguriert ist/wird.
Enabled	IPsec-Tunnel aktivieren/deaktivieren; ☐ Der IPsec-Tunnel ist nicht aktiv. ☒ Der IPsec-Tunnel ist aktiv.
Source Address	Quell-IP-Adresse und -Maske im CIDR-Format eingeben.
Destination Address	Ziel-IP-Adresse und -Maske im CIDR-Format eingeben.

Im WBM oder im WAGO Device Manager werden auf der Seite „IPsecClient“ unter „Gerätestatus/-aktionen“ folgende Informationen angezeigt.

Tabelle 74: „Gerätestatus/-aktionen“ – „IPsecTunnel“

Parameter	Bedeutung
IPsecTunnel Liste	Anzahl der aktivierten IPsec-Tunnel
IPsecTunnel <n>	Für jeden aktivierten IPsec-Tunnel wird ein eigener Bereich angezeigt.

Parameter	Bedeutung	
Established	Verbindungsstatus des IPsec-Tunnels	
	☐ false	Die Verbindung ist nicht aufgebaut.
	☒ true	Die Verbindung ist aufgebaut.

4.5.3 Netzwerkdienste

4.5.3.1 DHCP-Client

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

Folgende Parameter können bezogen werden:

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

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

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

4.5.3.2 SSH-Dienst

Der SSH-Dienst ist immer aktiv.

Die Kommunikation erfolgt über den Port 22.

Diese Einstellungen sind nicht veränderbar.

In der Werkseinstellung ist der Dienst von außen nicht erreichbar. Der Zugriff ist über alle Netzwerk-Schnittstellen blockiert.

Ein externer Zugriff ist möglich, wenn die Firewall-Regeln entsprechend eingestellt werden.

Der SSH-Dienst erlaubt nur eine passwortbasierte Authentifizierung.

Alle Authentifizierungsversuche werden unabhängig vom Erfolg geloggt.

Ein Login als „root“-Nutzer ist nicht möglich.

Andere Nutzer können aber zum „root“-Nutzer geändert werden, wenn dieser freigeschaltet ist.

Hinweise zur Bedeutung und Verwendung des „root“-Nutzers finden Sie im Abschnitt „Benutzerkonto ‚root‘“.

4.6 Speicherfunktionen

4.6.1 Automount

Tabelle 75: „Einstellungen“ – „Automount“

Parameter	Bedeutung
Enabled Storage Devices	Auswahlfeld mit möglichen Speichermedien und Anzeige der automatisch aktivierten Speichermedien; Im eingeklappten Zustand werden unterhalb des Auswahlfelds die automatisch aktivierten Speichermedien angezeigt. Im ausgeklappten Zustand wird eine Liste mit Kontrollfeldern für jedes verfügbare Speichermedium angezeigt.
☐	Das Speichermedien wird nicht automatisch aktiviert.
☒	Das Speichermedien wird automatisch aktiviert.
SDCards	Einstellung, ob SD-Karten automatisch aktiviert werden.

4.6.2 Datensicherung

Zur Sicherung und Wiederherstellung besitzt das Gerät eine Backup- und Restore-Funktion.

Hinweis

Firmwareversion beachten!

Das Wiederherstellen (Restore) ist nur möglich, wenn die Firmwareversionen zum Sicherungs- und Wiederherstellungszeitpunkt gleich sind.

Das Aulösen der Backup- und Restore-Funktionen werden im Ereignislog protokolliert.

4.6.2.1 Backup-Funktion

Mit der Backup-Funktion können die Einstellungen und die Benutzerdaten des Gerätes kopiert und in einer verschlüsselten Sicherungsdatei gespeichert werden.

Die Backup-Funktion kann mit dem WBM oder dem WAGO Device Manager ausgeführt werden.

Die Sicherung der Daten über die Backup-Funktion im WBM ist in Abschnitt „ **Backup durchführen** [► 91]“ beschrieben.

4.6.2.2 Restore-Funktion

Mit der Restore-Funktion können die Einstellungen und die Benutzerdaten aus einer verschlüsselten Sicherungsdatei in das Gerät kopiert und wiederhergestellt werden.

Die Sicherungsdatei wird vor dem Wiederherstellen auf Integrität geprüft. Schlägt diese Prüfung fehl, kann die Sicherungsdatei nicht eingespielt werden.

Nach erfolgreicher Integritätsprüfung wird die Wiederherstellung durch einen Neustart des Gerätes abgeschlossen.

Die Restore-Funktion kann mit dem WBM oder dem WAGO Device Manager ausgeführt werden.

Die Wiederherstellung der Daten über die Restore-Funktion im WBM ist in Abschnitt „[Re-store durchführen \[► 91\]](#)“ beschrieben.

4.7 Diagnosefunktionen

4.7.1 Diagnose über Anzeigeelemente

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

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

4.7.2 Diagnose über WBM oder WAGO Device Manager

4.7.2.1 Abbildung der LEDs

Im WBM oder im WAGO Device Manager werden in der Ansicht „Einstellungen“ auf der Seite „LEDs“ die Zustände der Geräte-LEDs abgebildet.

Zu jeder LED werden im Bereich „Gerätestatus/-aktionen“ folgende Angaben angezeigt:

- Der Name der LED entsprechend der Bedruckung auf dem Gerät
- Die Diagnoseinformation
- Die Farbe(n) entsprechend dem realen Zustand der LED auf dem Gerät

Einfarbige Flächen kennzeichnen dabei einen statischen Zustand der LED in der entsprechenden Farbe.

Mehrfarbige, überlagerte Flächen kennzeichnen einen Blinkzustand mit den entsprechenden Farben.

Eine graue Fläche entspricht dem Zustand „Aus“.

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

4.7.2.2 Verdrahtungstest (I/O-Check)

Über die Ansicht „I/O-Check“ kann ein einfacher Verdrahtungstest durchgeführt werden.

Dazu können die Zustände der Eingänge (soweit vorhanden oder konfiguriert) über die LED-Symbole oder im Klartext angezeigt werden (Monitoring-Modus).

Weiterhin können die Zustände der Ausgänge (soweit vorhanden oder konfiguriert) über die LED-Symbole oder im Klartext eingestellt werden (Control-Modus).

Die Bedienung ist im Abschnitt „[Verdrahtungstest durchführen \[► 96\]](#)“ beschrieben.

4.7.2.3 Ereignisprotokoll (Geräte-Log)

In der Ansicht „Geräte-Log“ können protokollierte Log-Einträge des Gerätes angezeigt werden.

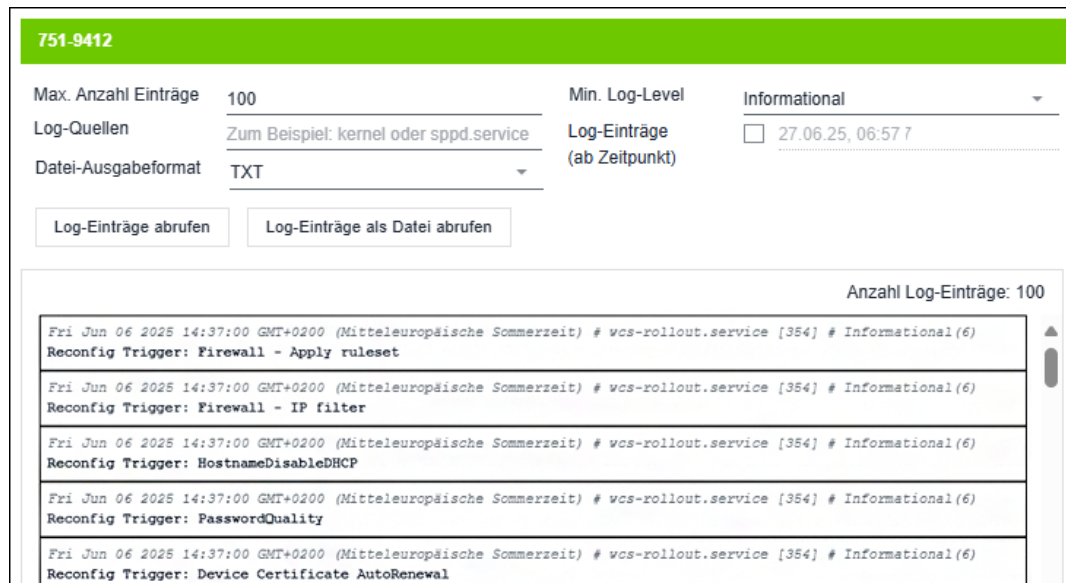
Über Anzeigefilter können vor dem Abrufen der Log-Einträge verschiedene Log-Level (Schweregrad der Meldung) zur Ansicht gewählt werden.

Die Sortierung der Einträge erfolgt nach Zeitstempel. Der neueste Eintrag befindet sich am unteren Ende der Liste.

Hinweis

Geräte-Log im Register „Einstellungen“ konfigurieren!

Welche Gerätemeldungen generell geloggt werden, konfigurieren Sie im Register „Einstellungen“ unter „Logging“. Das Register „Geräte-Log“ dient lediglich als Anzeige der konfigurierten Geräte-Logs und bietet zusätzliche Filtermöglichkeiten.



751-9412

Max. Anzahl Einträge: 100
 Log-Quellen: Zum Beispiel: kernel oder sppd.service
 Datei-Ausgabeformat: TXT
 Min. Log-Level: Informational
 Log-Einträge (ab Zeitpunkt): 27.06.25, 06:57 7

Log-Einträge abrufen Log-Einträge als Datei abrufen

Anzahl Log-Einträge: 100

Fri Jun 06 2025 14:37:00 GMT+0200 (Mittleuropäische Sommerzeit) # wcs-rollout.service [354] # Informational (6) Reconfig Trigger: Firewall - Apply ruleset
Fri Jun 06 2025 14:37:00 GMT+0200 (Mittleuropäische Sommerzeit) # wcs-rollout.service [354] # Informational (6) Reconfig Trigger: Firewall - IP filter
Fri Jun 06 2025 14:37:00 GMT+0200 (Mittleuropäische Sommerzeit) # wcs-rollout.service [354] # Informational (6) Reconfig Trigger: HostnameDisableDHCP
Fri Jun 06 2025 14:37:00 GMT+0200 (Mittleuropäische Sommerzeit) # wcs-rollout.service [354] # Informational (6) Reconfig Trigger: PasswordQuality
Fri Jun 06 2025 14:37:00 GMT+0200 (Mittleuropäische Sommerzeit) # wcs-rollout.service [354] # Informational (6) Reconfig Trigger: Device Certificate AutoRenewal

Abbildung 17: Register „Geräte-Log“

Option/Schaltfläche	Beschreibung
Max. Anzahl Einträge	Legt die maximale Anzahl der Einträge fest, die vom Gerät gelesen werden (standardmäßig 100). In diesem Register können maximal 1.000 Log-Einträge abgerufen und angezeigt werden. Beim Speichern in eine Datei lässt sich die Anzahl auf 100.000.000 Einträge erhöhen.
Min. Log-Level	Filtert die angezeigten Log-Einträge nach dem Log-Level.
Log-Quellen	Filtert die Log-Quellen der Log-Einträge nach der eingegebenen Zeichenkette und zeigt nur entsprechend passende Einträge an.
Log-Einträge (ab Zeitpunkt)	Bei Auswahl dieser Option können über einen Kalender das Datum und die Uhrzeit ausgewählt werden, ab welchem die Log-Einträge angezeigt werden. Auf diese Weise können die Ergebnisse beispielsweise auf die letzten 20 Minuten eingeschränkt werden.
Datei-Ausgabeformat	Sofern „Log-Einträge als Datei abrufen“ ausgewählt wird: Wählt das Ausgabeformat für die Datei, in der Log-Einträge gespeichert werden. Zur Verfügung stehen das Textformat „TXT“ oder das Tabellenformat „CSV“.
[Log-Einträge abrufen]	Zeigt die Log-Einträge basierend auf der Konfiguration und entsprechend der gewählten Filter an.
[Log-Einträge als Datei abrufen]	Öffnet einen Dateixplorer zum Speichern der Log-Einträge basierend auf der Konfiguration und entsprechend der gewählten Filter.
Inhalt der Tabelle	Zeigt für jeden Log-Eintrag folgende Informationen an: Zeitstempel (Erstellungszeitpunkt des Eintrages), Quelle (Service/Dienst, welcher den Log-Eintrag erstellt hat), Log-Level (Schweregrad des Eintrages) sowie ggf. weitere Informationen, abhängig von Quelle/Dienst Die Sortierung der Einträge erfolgt nach Zeitstempel von alt (oben) nach neu (unten).

Weitere Informationen finden Sie im Abschnitt „[Geräte-Log einsehen \[► 97\]](#)“.

5 In Betrieb nehmen

5.1 Einschalten des Controllers

Überprüfen Sie vor Einschalten des Controllers, dass Sie

- den Controller ordnungsgemäß montiert haben (siehe Produkthandbuch, Abschnitt „Montieren“),
- alle benötigten Datenleitungen (siehe Produkthandbuch, Abschnitt „Anschlüsse“) an die entsprechenden Schnittstellen angeschlossen haben,
- die Spannungsversorgung (siehe Produkthandbuch, Abschnitt „Anschlüsse“) angeschlossen haben,
- 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 aller LEDs signalisiert.

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

Gleichzeitig wird das Laufzeitsystem CODESYS V3 gestartet.

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

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

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

5.2 Einstellen einer IP-Adresse

Im Auslieferungszustand des Controllers gelten für die ETHERNET-Kommunikation folgende Voreinstellungen.

Tabelle 76: Voreinstellung ETHERNET-Kommunikation

Schnittstelle	Voreinstellung
ETHERNET-Ports X1/X2	▪ Switched Mode (Bridge 1) ▪ Dynamische Vergabe der IP-Adresse mittels DHCP ▪ Voreingestellte statische IP-Adresse: 172.29.233.42/24
USB-Service-Schnittstelle	Festeingestellte statische IP-Adresse: 192.168.42.42

- Passen Sie mit einem Konfigurationswerkzeug (z. B. WBM oder WAGO Device Manager) die IP-Adressierung der ETHERNET-Ports X1/X2 an Ihre Systemstruktur an, siehe [Konfigurieren \[► 84\]](#).
- ➔ Alle erforderlichen Netzwerkteilnehmer befinden sich im gleichen Subnetz und können miteinander kommunizieren

5.2.1 Einstellen einer IP-Adresse über das WBM

Die erforderlichen Einstellungen finden Sie im Register „Einstellungen“ auf der Seite „Network“.

1. Wählen Sie in der Gruppe „Bridge Configuration“ die Zuordnung der Ports aus.
2. Tragen Sie in der Gruppe „Bridge <n>“ die entsprechende IP-Adresse(n) ein

5.2.2 Zuweisen einer IP-Adresse mit DHCP

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

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

In Verbindung mit einem an das DHCP 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 Produktes ist auf dem seitlich am Produkt angebrachten Etikett aufgedruckt.

5.3 Passwörter ändern

Bei der ersten Anmeldung oder auf Veranlassung durch den Administrator werden Sie im Anmeldefenster aufgefordert, ein neues Passwort festzulegen oder Ihr vorhandenes Passwort zu ändern.

1. Geben Sie ggf. das alte Passwort ein.
2. Geben Sie das neue Passwort ein.
3. Wiederholen Sie das neue Passwort.

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

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

Hinweis

Zulässige Zeichen für Passwörter

Passwörter dürfen nur die folgenden Zeichen enthalten:

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

Die Mindestanzahl der jeweiligen Zeichen ist über das WBM oder den WAGO Device Manager einstellbar.

Tabelle 77: „Einstellungen“ – „Accountmanagement/PasswordQuality“

Parameter	Bedeutung
Min Length	Eingabe der Mindestlänge des Passworts (6 ... 100, Werkseinstellung = 8)

Parameter	Bedeutung
Min Capital	Eingabe der Mindestanzahl von Großbuchstaben (A ... Z) (0 ... 100, Werkseinstellung = 1)
Min Lowercase	Eingabe der Mindestanzahl von Kleinbuchstaben (a ... z) (0 ... 100, Werkseinstellung = 1)
Min Digit	Eingabe der Mindestanzahl von Ziffern (0 ... 9) (0 ... 100, Werkseinstellung = 1)
Min Special	Eingabe der Mindestanzahl von Sonderzeichen () (0 ... 100, Werkseinstellung = 1)

5.4 Benutzer verwalten

5.4.1 Lokale Benutzerrollen und -konten verwalten

Lokale Benutzerrollen und -konten werden im WBM oder im WAGO Device Manager auf der Seite „AccountmanagementLocal“ verwaltet.

Für die Anzeige der lokalen Benutzerverwaltung ist das Benutzerrecht „StaticPermission 3041 (wdx-accountmanagementlocal-ro)“ erforderlich.

Für eine Anpassung der lokalen Benutzerverwaltung ist das Benutzerrecht „StaticPermission 3040 (wdx-accountmanagementlocal-rw)“ erforderlich.

Der Systembenutzer „admin“ verfügt über beide Berechtigungen.

Die vordefinierte Benutzerrolle „RBAC-Admin“ verfügt in der Werkseinstellung ebenfalls über beide Berechtigungen.

- ✓ Sie sind als Benutzer mit der erforderlichen Berechtigung am Controller angemeldet.
- Markieren Sie das Kontrollfeld „Enabled“ im Bereich „Accountmanagement/Local“, um das lokale Benutzermanagement zu aktivieren.

5.4.1.1 Lokale Benutzerkonten verwalten

Im Bereich „User Liste“ werden die angelegten Benutzerkonten mit ihren Rollen angezeigt.

Ein neues Benutzerkonto anlegen

1. Klicken Sie auf die Schaltfläche **[+User]** am Ende der Liste.
 - ⇒ Ein neuer Bereich „User <n>“ wird angezeigt.
2. Geben Sie im Eingabefeld „Name“ den gewünschten Namen für das Benutzerkonto ein.
3. Aktivieren oder deaktivieren Sie das Benutzerkonto im Kontrollfeld „Enabled“.
4. Klicken Sie im Auswahlfeld „Roles“ die gewünschten Benutzerrollen an.
 - ⇒ Die ausgewählten Benutzerrollen werden im Auswahlfeld grau hinterlegt und in die Liste eingetragen.
5. Wenn Sie eine Benutzerrolle wieder aus der Liste entfernen möchten, klicken Sie auf die Schaltfläche **[x]** neben der entsprechenden Benutzerrolle. Alternativ klicken Sie die entsprechende, grau hinterlegte Benutzerrolle im Auswahlfeld erneut an.
 - ⇒ Die entsprechenden Benutzerrollen werden aus der Liste gelöscht.
6. Markieren Sie das Kontrollfeld „Force Password Change“, wenn der neue Benutzer beim ersten Einloggen sein Passwort ändern muss.

7. Klicken Sie nach der Zuordnung aller gewünschten Benutzerrollen auf die Schaltfläche **[Ins Gerät schreiben]**.

➔ Das neue Benutzerkonto ist angelegt und kann, wenn aktiviert, verwendet werden.

Ein Benutzerkonto ändern

1. Navigieren Sie zu dem zu ändernden Benutzerkonto.
2. Ändern Sie ggf. im Eingabefeld „Name“ den Namen für das Benutzerkonto.
3. Aktivieren oder deaktivieren Sie ggf. das Benutzerkonto im Kontrollfeld „Enabled“.
4. Fügen Sie Benutzerrollen hinzu oder entfernen Sie bestehende Benutzerrollen, wie oben beschrieben.
5. Ändern Sie ggf. die Einstellung im Kontrollfeld „Force Password Change“, wenn eine Passwortänderung beim nächsten Einloggen erforderlich ist oder nicht.
6. Klicken Sie nach dem Ändern der Einstellungen auf die Schaltfläche **[Ins Gerät schreiben]**.

➔ Das Benutzerkonto ist geändert.

Ein Benutzerkonto entfernen

1. Navigieren Sie zu dem zu löschenden Benutzerkonto.
2. Klicken Sie auf die Schaltfläche **[Mülleimer]** in der Kopfzeile des Kontoeintrags.
⇒ Das Benutzerkonto wird aus dem Bereich „User Liste“ entfernt.
3. Klicken Sie nach dem Entfernen des Benutzerkontos auf die Schaltfläche **[Ins Gerät schreiben]**.

➔ Das Benutzerkonto ist endgültig entfernt und kann nicht mehr verwendet werden.

5.4.1.2 Lokale Benutzerrollen verwalten

Im Bereich „UserRole Liste“ werden die angelegten Benutzerrollen mit ihren Berechtigungen angezeigt.

Eine neue Benutzerrolle anlegen

1. Klicken Sie auf die Schaltfläche **[+UserRole]** am Ende der Liste.
⇒ Ein neuer Bereich „UserRole <n>“ wird angezeigt.
2. Geben Sie im Eingabefeld „Name“ den gewünschten Namen für die Benutzerrolle ein.
3. Klicken Sie im Auswahlfeld „Permissions“ die gewünschten Berechtigungen an.
⇒ Die ausgewählten Berechtigungen werden im Auswahlfeld grau hinterlegt und in die Liste eingetragen.
4. Wenn Sie eine Berechtigung wieder aus der Liste entfernen möchten, klicken Sie auf die Schaltfläche **[x]** neben der entsprechenden Berechtigung. Alternativ klicken Sie die entsprechende, grau hinterlegte Berechtigung im Auswahlfeld erneut an.
⇒ Die entsprechenden Berechtigungen werden aus der Liste gelöscht.
5. Klicken Sie nach der Zuordnung aller gewünschten Berechtigungen auf die Schaltfläche **[Ins Gerät schreiben]**.

➔ Die neue Benutzerrolle ist angelegt und kann in den Benutzerkonten verwendet werden.

Eine Benutzerrolle ändern

1. Navigieren Sie zu der zu ändernden Benutzerrolle.
 2. Ändern Sie ggf. im Eingabefeld „Name“ den Namen für die Benutzerrolle.
 3. Fügen Sie Berechtigungen hinzu oder entfernen Sie bestehende Berechtigungen, wie oben beschrieben.
 4. Klicken Sie nach dem Ändern der Einstellungen auf die Schaltfläche **[Ins Gerät schreiben]**.
- ➔ Die Benutzerrolle ist geändert.

Eine Benutzerrolle entfernen

1. Navigieren Sie zu der zu löschenden Benutzerrolle.
 2. Klicken Sie auf die Schaltfläche **[Mülleimer]** in der Kopfzeile des Rolleneintrags.
⇒ Die Benutzerrolle wird aus dem Bereich „UserRole Liste“ entfernt.
 3. Klicken Sie nach dem Entfernen der Benutzerrolle auf die Schaltfläche **[Ins Gerät schreiben]**.
- ➔ Die Benutzerrolle ist endgültig entfernt und kann nicht mehr verwendet werden.

5.5 Ausschalten/Neustart

Um den Controller auszuschalten, schalten Sie die Versorgungsspannung ab.

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

Hinweis

Neustart nach Parameteränderungen nicht durch Aus- und Wiedereinschalten hervorrufen!

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

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

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

6 Konfigurieren

6.1 Konfigurieren im WBM

- ✓ Das Gerät ist über das Netzwerk oder per USB erreichbar.
- 1. Öffnen Sie den Browser und geben Sie die IP-Adresse des Controllers ein.
 - ⇒ Das WBM wird geöffnet und eine Login-Nachricht angezeigt.
- 2. Klicken Sie auf die Schaltfläche **[Loginfenster öffnen]**.
 - ⇒ Das Loginfenster wird geöffnet.
- 3. Geben Sie Ihre Zugangsdaten (Username und Passwort) ein und klicken Sie auf die Schaltfläche **[Login]**.
 - ⇒ Nach erfolgreicher Anmeldung können Sie im WBM navigieren.
- 4. Öffnen Sie die Ansicht „Einstellungen“.
Sehen Sie sich zur Verwendung der Ansicht „Einstellungen“ die Tipps unten an.
 - ⇒ Die Gerätedaten werden nach dem Verbindungsaufbau automatisch ausgelesen und zunächst als Zielwerte (links) übernommen, so dass sich aktuelle Gerätewerte und Zielwerte zunächst entsprechen.
- 5. Wählen Sie ein Register aus, in welchem Sie Einstellungen vornehmen möchten, z. B. „VPN“.
- 6. Führen Sie Ihre Änderungen in der Spalte „Zielwerte“ durch. Setzen Sie beispielsweise „OpenVPN“ auf „Enabled“.
 - ⇒ Ihnen wird mit einem Ungleichzeichen angezeigt, dass sich der Zielwert nun von dem aktuellen Wert des Gerätes unterscheidet.
- 7. Führen Sie bei Bedarf weitere Änderungen in verschiedenen Registern durch.
 - ⇒ Eine Übersicht, in welchem Register Sie Änderungen vorgenommen haben, finden Sie im Dropdown-Menü im oberen Bereich. Aus diesem Menü können Sie bei Bedarf direkt zu dem Register wechseln, in welchem Sie die Änderungen durchgeführt haben. Auch die entsprechenden Register selbst werden nach Änderungen mit einem Ungleichzeichen versehen.
- 8. Um die Änderungen auf das Gerät zu übertragen, klicken Sie unter den geänderten Werten auf **[Ins Gerät schreiben ►]**.
 - ➔ Konfigurationen und Parameter wurden auf das Gerät übertragen. Der Knoten ist einsatzbereit.

Tipps

- Unter Einstellungen finden Sie eine Beschreibung der Ansicht „Einstellungen“ mit Erläuterungen zu Icons, Bedienelementen und zum Dateihandling.
- Setzen Sie einen Haken in der Checkbox „Nur relevante anzeigen“, um nur diejenigen Einstellungen anzuzeigen, die relevant für die verwendete Konfiguration sind. Ausgegraute, und damit nicht änderbare, irrelevante Einstellungen werden in dem Fall ausgeblendet.
- Verwenden Sie das Aktualisieren-Icon , um aktuelle Werte aus dem Gerät zu lesen und anzuzeigen. Eine Aktualisierung der Werte erfolgt ansonsten bei jedem Verbindungsaufbau und beim Ausführen von Schreiboperationen.

Aktionen direkt ausführen

Es gibt Änderungen, die Sie nicht als Zielwert speichern und dann übertragen müssen, sondern die direkt an das Gerät gesendet werden, z. B. die Änderung der Systemzeit.

Sie finden solche Aktionen im unteren Bereich der jeweiligen Register unter „Gerätestatus/-aktionen“. In demselben Bereich finden Sie auch Statusinformationen des Gerätes.

7 Service

7.1 Firmwareänderungen

! ACHTUNG

Controller nicht ausschalten!

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

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

i Hinweis

Zur Firmwarezielversion passende Dokumentation bereithalten!

Durch eine Firmwareänderung können Eigenschaften und Funktionen des Controllers verändert, entfernt oder hinzugefügt werden. Damit können ggf. in dieser Dokumentation beschriebene Eigenschaften und Funktionen nicht zur Verfügung stehen oder Eigenschaften oder Funktionen des Controllers in dieser Dokumentation nicht beschrieben sein.

1. Verwenden Sie daher nach einer Firmwareänderung nur die zur Zielfirmware passende Dokumentation.
2. Bei Rückfragen wenden Sie sich an den WAGO Support.

Sie können die Firmware über das WBM aktualisieren.

7.1.1 Firmware-Update mit WBM durchführen

Möchten Sie das Gerät mit einer anderen Firmwareversion verwenden, als der eingestellten, dann können Sie die Firmwareversion über die Oberfläche ändern.

! ACHTUNG

Um Geräteschäden zu vermeiden, Hinweise beachten!

Durch eine Unterbrechung des Updatevorganges kann das Gerät beschädigt werden. Beachten Sie aus diesem Grund die folgenden Hinweise bezüglich Hardware und Software.

Hinweise Hardware

- Schalten Sie Geräte nicht aus.
- Unterbrechen Sie nicht die Spannungsversorgung der Geräte.
- Entfernen Sie Geräte nicht aus dem Verbund eines Knotens.
- Stellen Sie sicher, dass die Kommunikation mit dem Gerät während des Updates nicht unterbrochen wird.
- Falls Sie das Update über die Serviceschnittstelle vornehmen, trennen Sie zuvor das Feldbuskabel vom Gerät.
- Beenden Sie die Software nicht während des Vorganges.

Hinweise Software

- Halten Sie die Applikation auf dem Gerät an, bevor Sie ein Update durchführen.
- Durch das Update können Programme und Daten im Gerät verloren gehen. Vergewissern Sie sich, dass Sie eine aktuelle Sicherung dieser Daten besitzen.
- Die Applikation sowie andere Dateien aus dem Speicher oder dem Dateisystem müssen nach dem Update neu auf den Controller übertragen werden.
- Notieren Sie nach dem Ersetzen der Firmware den neuen Firmwarestand (xx) in dem dafür vorgesehenen Kästchen auf dem Controller.

Hinweis

Haftungsausschluss bei Updates!

Haftungsansprüche gegenüber der WAGO GmbH & Co. KG, die sich auf Schäden materieller oder ideeller Art beziehen, welche durch Updates (z. B. Firmwareänderungen) entstehen, sind ausgeschlossen. Die Nutzung erfolgt ausschließlich auf Risiko des Anwenders.

Hinweis

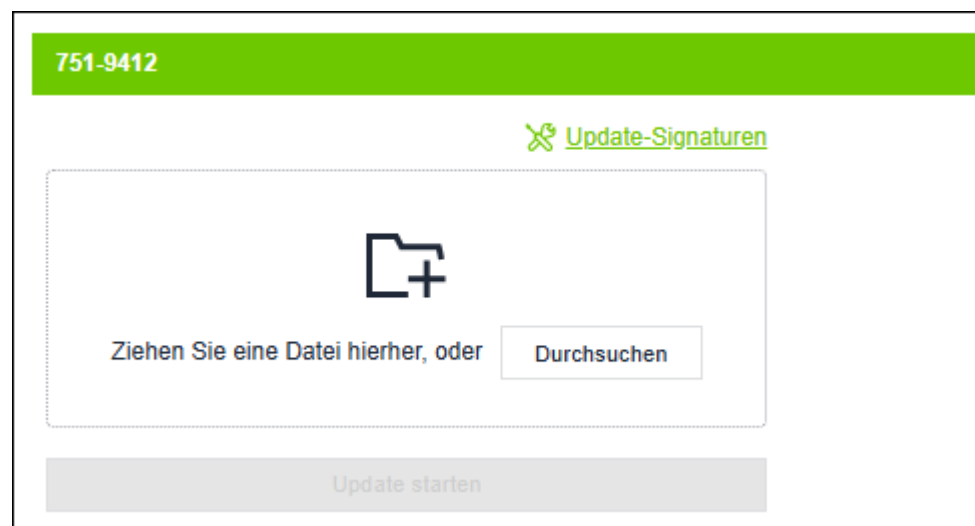
Weitere Informationen beim WAGO Support!

Weitere Informationen zu Updates/Firmwareänderungen erhalten Sie beim Support der WAGO GmbH & Co. KG.

Hinweis

Updates können einige Minuten dauern!

Beachten Sie, dass Updates, z. B. das Ersetzen der Firmware, je nach Hardwareausstattung des Gerätes einige Minuten dauern kann.



- ✓ Sie haben im  **WAGO Download Center** eine neue Updatedatei für Ihr Gerät heruntergeladen oder laden diese im Folgenden direkt aus dem WAGO Download Center.
- ✓ **Hinweis: Eigene Firmware erfordert entsprechende Zertifikate!**
Firmwaredateien müssen signiert sein. Für WAGO Firmware, die Sie im WAGO Navigator/ WAGO Download Center herunterladen, ist dies bereits der Fall. Falls Sie jedoch Firmwa-

re mit eigenen oder mehreren Komponenten laden, klicken Sie auf „Update-Signaturen“ und fügen auf der Seite entsprechende, eigene Zertifikate hinzu, mit welchen die Signatur des gesamten Firmwareupdates geprüft wird. Ohne Zertifikat ist ein Firmwareupdate nicht möglich.

1. Klicken Sie im Menüband auf **[Update]**.
 2. Ziehen Sie die Updatedatei auf den Ablagebereich.
Alternativ klicken Sie auf **[Durchsuchen]** und wählen die heruntergeladene Updatedatei aus.
 - ⇒ Der Dateiname der gewählten Updatedatei wird angezeigt. Über **[Andere Datei wählen]** können Sie bei Bedarf die Updatedatei wechseln.
 3. Klicken Sie auf **[Update starten]**.
 - ⇒ Die Updatedatei wird zunächst auf das Gerät geladen. Anschließend wird das Update ausgeführt.
 - ⇒ Der Update-Vorgang kann einige Zeit (ca. 20 min) dauern. Während des Vorganges stehen andere Prozesse und die Bedienung des WBM nicht zur Verfügung. Die Verbindung zum Gerät kann zeitweise unterbrochen werden.
 - ⇒ Nach dem Update wird das Gerät neu gestartet.
 4. Klicken Sie auf **[WBM neu laden]**.
 5. Melden Sie sich mit den Zugangsdaten an Ihrem Gerät an.
 - ⇒ Falls Fehler aufgetreten sind, wird Ihnen dies im Meldungsfenster und im Register „Update“ angezeigt.
- ➔ Das Gerät läuft mit der neuen Firmware.

7.2 Reset-Funktionen auslösen

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

7.2.1 Warmstart-Reset

Bei einem Warmstart-Reset werden alle CODESYS V3-Applikationen zurückgesetzt. Alle globalen Daten werden auf ihre Initialisierungswerte gesetzt. Dies entspricht dem CODESYS V3-IDE-Befehl „Reset warm“.

- Um einen Warmstart-Reset durchzuführen, bringen Sie den Betriebsartenschalter in die Reset-Position und halten ihn dort länger als 2 Sekunden aber kürzer als 7 Sekunden.
- ➔ Die Ausführung wird durch ein kurzes Erlöschen der roten „RUN“-LED nach dem Loslassen des Betriebsartenschalters signalisiert.

7.2.2 Kaltstart-Reset

Bei einem Kaltstart-Reset werden alle CODESYS V3-Applikationen zurückgesetzt. Alle globalen Daten und die Retain-Variablen werden auf ihre Initialisierungswerte gesetzt. Dies entspricht dem CODESYS V3-IDE-Befehl „Reset kalt“.

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

7.2.3 Software-Reset (Neustart)

Bei einem Software-Reset wird das Produkt neu gestartet.

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

7.2.4 Factory-Reset

! ACHTUNG

Controller nicht ausschalten!

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

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

i Hinweis

Alle Parameter und Passwörter werden überschrieben!

Mit dem Reset werden alle Parameter und Passwörter überschrieben.

Gespeicherte Boot-Projekte einschließlich vorhandener Webvisualisierungsdaten werden gelöscht.

Nachinstallierte Firmwarefunktionen werden gelöscht.

Softwarelizenzen werden gelöscht.

- Bei Rückfragen wenden Sie sich an den WAGO Support.

Um einen „Factory-Reset“ durchzuführen, gehen Sie wie folgt vor:

1. Betätigen Sie den Reset-Taster und halten Sie ihn gedrückt.
 2. Schieben Sie den Betriebsartenschalter in die Position „RESET“ und halten Sie ihn in dieser Position.
 3. Halten Sie beide Taster, bis nach ca. 8 Sekunden die „SYS“-LED im Wechsel orange/grün blinkt.
 4. Wenn die „SYS“-LED im Wechsel orange/grün blinkt, lassen Sie den Betriebsartenschalter und den Reset-Taster los.
- ➔ Der Controller wurde zurückgesetzt und führt einen automatischen Neustart aus.

Alternativ können Sie einen „Factory-Reset“ auch über das WBM oder den WAGO Device-Manager durchzuführen. Gehen Sie dazu wie folgt vor:

1. Verbinden Sie den Controller über eine ETHERNET-Schnittstelle oder über die USB-Service-Schnittstelle mit Ihrem PC.
2. Öffnen Sie das WBM auf dem Controller oder den WAGO Device-Manager auf dem PC.
3. Melden Sie sich mit Ihrem Benutzer und Passwort auf dem Controller an.
4. Öffnen Sie das Register „System“.
5. Navigieren Sie zum Eintrag „Factory Reset“.
6. Klicken Sie im Bereich „Gerätestatus/-aktionen“ auf die Schaltfläche **[Reset]**.
⇒ Ein Dialog mit einer Sicherheitsabfrage wird geöffnet.
7. Klicken Sie auf die Schaltfläche **[Werkseinstellungen wiederherstellen]**.
➔ Der Controller wird zurückgesetzt und führt einen automatischen Neustart aus.

7.3 CODESYS Applikationen starten/stoppen

CODESYS Applikationen können mit dem Betriebsartenschalter oder über die CODESYS Programmieroberfläche gestartet oder gestoppt werden.

Über die CODESYS Programmieroberfläche können die CODESYS Applikationen nur gestartet werden, wenn der Betriebsartenschalter in Position „RUN“ steht.

Das Starten oder Stoppen der CODESYS Applikationen wird im Logsystem erfasst (Ereignis-logging).

7.3.1 CODESYS Applikationen starten

- Bringen Sie den Betriebsartenschalter in die Position „RUN“.
- ➔ Die CODESYS Applikationen werden gestartet.
- ➔ Die LED „RUN“ leuchtet grün.

7.3.2 CODESYS Applikationen stoppen

- Bringen Sie den Betriebsartenschalter in die Position „STOP“.
- ➔ Alle CODESYS Applikationen werden gestoppt.
- ➔ Die LED „RUN“ erlischt.

Die CODESYS Applikationen können nicht über die CODESYS Programmieroberfläche gestartet werden, wenn der Betriebsartenschalter in Position „STOP“ steht.

7.4 Daten sichern und wiederherstellen

Hinweis

Firmwareversion beachten!

Das Wiederherstellen (Restore) ist nur möglich, wenn die Firmwareversionen zum Sicherungs- und Wiederherstellungszeitpunkt gleich sind.

7.4.1 Backup durchführen

1. Klicken Sie im Menüband auf **[Backup/Restore]**.
 2. Wählen Sie im Auswahlfeld „Ablageort“ aus, in welchem Netzwerk-/PC-Ordner oder auf welchem Wechselmedium das Backup abgelegt werden soll.
 3. Geben Sie unter „Backup“ das Passwort ein, mit welchem Sie die Backup-Datei verschlüsselt speichern möchten und wiederholen Sie die Passworteingabe.
 - ⇒ **Hinweis: Bewahren Sie Ihr Passwort sorgfältig auf!**
Das Passwort wird zwingend für die Wiederherstellung des Backups benötigt. Ohne das korrekte Passwort ist ein Zugriff auf die gesicherten Daten nicht mehr möglich.
 - ⇒ **Hinweis: Backup-Datei und Passwort vor unbefugtem Zugriff schützen!**
Mit Kenntnis des Passwortes und Zugang zur Backup-Datei ist eine indirekte Änderung der Gerätekonfiguration möglich.
 4. Klicken Sie auf **[Backup-Vorgang starten]**.
 - ⇒ Einstellungen und Nutzerdaten sowie die CODESYS Applikation werden als Backup auf dem Gerät zusammengestellt und anschließend als Backup-Datei (*.7zip) von dem Gerät auf den Engineering-PC geladen. Eine Prozentanzeige zeigt Ihnen an, wann der Download abgeschlossen ist.
 - ⇒ Sofern Ihr Browser nicht anders konfiguriert ist, finden Sie die heruntergeladene Datei in Ihrem „Downloads“-Ordner (browserabhängig).
- ➔ Der Backup-Vorgang ist beendet.

7.4.2 Restore durchführen

Beachten Sie für die Rücksicherung Ihrer Daten die folgenden Hinweise:

- Der Restore-Vorgang kann einige Minuten dauern. Nach dem Restore-Vorgang wird das Gerät neu gestartet und ist danach wieder einsatzbereit.
 - Beachten Sie, dass Gerätedaten entsprechend der Inhalte des gewählten Backups überschrieben werden. Wenn Sie nach der Backup-Erstellung verbindungsrelevante Daten ändern (z. B. die IP-Adresse), kann bei einem automatischen Neustart während des Restore-Vorganges eventuell keine Verbindung mehr zum Gerät aufgebaut werden.
 - Stellen Sie sicher, dass Sie über ggf. geänderte Zugangsdaten (Benutzer/Passwort) für das Gerät verfügen.
 - Stellen Sie sicher, dass das Gerät während des Restore-Vorganges und auch danach physikalisch erreichbar ist: Es muss für die gesamte Zeit des Restore-Vorganges eine Netzwerkverbindung über ein geeignetes Medium (z. B. Kabel, WLAN) bestehen.
 - Stellen Sie sicher, dass Sie ggf. geänderte IP-Adressen/Geräteadressen/DHCP-Server-Adressen zur Hand haben.
 - Die Wiederherstellung der Daten kann fehlschlagen, wenn der freie Speicherbereich auf dem Gerät nicht ausreicht.
1. Klicken Sie im Menüband auf **[Backup/Restore]**.
 2. Wählen Sie im Bereich „Restore“ die Quelle Ihrer Backup-Datei aus.
 - ⇒ Falls Sie das Dateisystem als Quelle wählen, wird ein Ablagebereich  eingeblendet.
 3. Geben Sie unter „Restore“ das Passwort ein, mit dem Sie die Backup-Datei gesichert haben.

4. Ziehen Sie die Backup-Datei (*.7zip) auf den Ablagebereich.
Alternativ klicken Sie auf **[Durchsuchen]** und wählen eine Backup-Datei aus.
⇒ Der Dateiname der gewählten Backup-Datei wird angezeigt. Über **[Andere Datei wählen]** können Sie bei Bedarf die Backup-Datei wechseln.
5. Um die Daten aus der gewählten Backup-Datei wiederherzustellen, klicken Sie auf **[Restore-Vorgang starten]**.
⇒ Zunächst wird die Backup-Datei auf das Gerät geladen. Im Folgenden startet automatisch der Restore-Vorgang auf dem Gerät.
Ihnen wird angezeigt, wenn die Wiederherstellung erfolgreich war.
⇒ Falls das Gerät beispielsweise aufgrund geänderter IP-Daten nicht mehr erreichbar sein sollte, werden Sie aufgefordert, das WBM des Gerätes mit der neuen IP-Adresse manuell im Browser zu öffnen.
→ Der Restore-Vorgang ist abgeschlossen.

7.5 WDX-Methoden für Fertigung

Die WDX-Methoden

- Manufacturing/ExecuteCommand "CODESYSLicense" <Lizenzdatei>
- Manufacturing/ExecuteCommand "DeviceIdentityCert" <PEM-Zertifikat>

sind nur für die Fertigung anwendbar. Sie können nur einmal aufgerufen werden.

Ein wiederholter Aufruf durch Standardbenutzer ist nicht möglich und führt zu einer Fehlermeldung!

7.6 Zertifikate erstellen und verwalten

7.6.1 Gerätezertifikate erstellen

Gerätezertifikate (Zertifikatsdateien und zugehörige private Schlüsseldateien) können auf zwei Wegen erstellt werden:

1. Direkt auf dem Controller mit anschließender Signierung über eine externe PKI.
2. Über einen verbundenen Enrollment-Server mit automatischer Signierung.

7.6.1.1 Selbstsignierte Zertifikate

Selbstsignierte Gerätezertifikate (Zertifikatsdatei und die zugehörige private Schlüsseldatei) können direkt auf dem Controller generiert werden.

Selbstsignierte Gerätezertifikate können anschließend manuell über eine externe PKI signiert werden.

Um eine selbstsignierte Zertifikatsdatei und die zugehörige private Schlüsseldatei zu generieren und anschließend manuell über eine externe PKI zu signieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie im WBM oder im WAGO Device-Manager die Seite „Device Certificates“.

2. Klicken Sie im Bereich „Gerätestatus/-aktionen“ auf die Schaltfläche **[Create Certificate]**.
 - ⇒ Das Popup-Fenster „CertStore/Device/CreateCertificate“ wird geöffnet.
 3. Wählen Sie im Dropdown-Feld „KeyType“ den Schlüsseltyp (RSA:2048/RSA:4096 / EC:prime256v1) aus.
 4. Geben Sie im Feld „DistinguishedName“ einen Namen für das Zertifikat ein. Dieser Name wird bei der Auflistung der Zertifikate als Kommentar angezeigt. Die Syntax des Namens ist gemäß „RFC 4514“ vorgegeben. Bei der Eingabe wird eine Hilfe angezeigt.
 5. Klicken Sie auf die Schaltfläche **[Create Certificate]**.
 6. Schließen Sie das Popup-Fenster.
 - ⇒ Das generierte Zertifikat wird im Bereich „Einstellungen“ in der Spalte „Aktuelle Werte“ als neuer Eintrag „DeviceCertificate <n> (<Name>)“ mit dem aus dem Feld „DistinguishedName“ übernommenen Namen angezeigt.
 7. Klicken Sie auf die Schaltfläche **[Als Zielwerte übernehmen]**.
 - ⇒ Das Zertifikat wird in der Spalte „Zielwerte“ angezeigt.
 8. Klicken Sie im Bereich „Gerätestatus/-aktionen“ bei dem soeben generierten Zertifikat auf die Schaltfläche **[Create Signing Request]**.
 - ⇒ Das Popup-Fenster „CertStore/Device/Certificates/2/CreateSigningRequest“ wird geöffnet.
 9. Geben Sie im Feld „DistinguishedName“ noch einmal den Namen für das zu signierende Zertifikat ein.
 10. Klicken Sie auf die Schaltfläche **[Create Signing Request]**.
 - ⇒ Der Status wird angezeigt und es wird eine Zertifikatsdatei in Textform ausgegeben.
 11. Kopieren Sie diese Textdatei zur Signierung über der externe PKI.
 12. Wenn die Zertifikatsdatei erfolgreich signiert ist, laden Sie diese Datei wieder in den Controller.
 13. Öffnen Sie dazu das Dropdown-Menü bei der Größenangabe.
 14. Wählen Sie den Menüpunkt **[Auswählen]**.
 - ⇒ Ein Dateimanager-Fenster wird geöffnet.
 15. Navigieren Sie zu der signierten Datei und importieren Sie diese.
 16. Klicken Sie auf die Schaltfläche **[Ins Gerät schreiben]**, um die Änderung zu übernehmen.
 - ⇒ Das Zertifikat wird im Bereich Gerätestatus/-aktionen mit dem aus dem Feld „DistinguishedName“ übernommenen Namen angezeigt.
- ➔ Das Zertifikat kann jetzt verwendet werden.

7.6.1.2 Über eine externe PKI signierte Zertifikate

Gerätezertifikate (Zertifikatsdatei und die zugehörige private Schlüsseldatei) können generiert und automatisch über eine externe PKI signiert werden, wenn der Controller mit einem Enrollment-Server verbunden ist.

Um eine Verbindung zu einem Enrollment-Server herzustellen, gehen Sie folgendermaßen vor:

1. Öffnen Sie im WBM oder im WAGO Device-Manager die Seite „Device Certificates“.

2. Geben Sie Bereich „Einstellungen“ in der Gruppe „CertStore/EnrollmentServer“ den Hostnamen des Servers und die Authentifizierungsdaten ein.
 3. Stellen Sie im Kontrollfeld „Verbose“ ein, ob bei der Verbindung ein ausführliche Protokollierung erfolgen soll.
 4. Wählen Sie im Auswahlfeld „CA Certificate“ ein Root-Zertifikat aus, um die Verbindung zu verifizieren.
 5. Klicken Sie auf die Schaltfläche **[Ins Gerät schreiben]**, um die Einstellungen im Controller zu übernehmen.
- ➔ Die Einstellungen werden in der Spalte „Aktuelle Werte“ angezeigt.

Um eine Zertifikatsdatei und die zugehörige private Schlüsseldatei zu generieren und automatisch über eine externe PKI zu signieren, gehen Sie folgendermaßen vor:

1. Klicken Sie im Bereich „Gerätestatus/-aktionen“ auf die Schaltfläche **[Create Certificate with Enrollment]**.
 - ⇒ Das Popup-Fenster „CertStore/Device/CreateCertificateWithEnrollment“ wird geöffnet.
 2. Wählen Sie im Dropdown-Feld „KeyType“ den Schlüsseltyp („RSA:2048“/„RSA:4096“/„EC:prime256v1“) aus.
 3. Geben Sie im Feld „DistinguishedName“ einen Namen für das Zertifikat ein. Dieser Name wird bei der Auflistung der Zertifikate als Kommentar angezeigt. Die Syntax des Namens ist gemäß „RFC 4514“ vorgegeben. Bei der Eingabe wird eine Hilfe angezeigt.
 4. Geben Sie die Authentifizierungsdaten („AuthUser“ und „AuthPassword“) für den Enrollment-Server ein.
 5. Klicken Sie auf die Schaltfläche **[Create Certificate with Enrollment]**.
 6. Schließen Sie das Popup-Fenster.
 - ⇒ Das generierte Zertifikat wird im Bereich „Einstellungen“ in der Spalte „Aktuelle Werte“ als neuer Eintrag „DeviceCertificate <n> (<Name>)“ mit dem aus dem Feld „DistinguishedName“ übernommenen Namen angezeigt.
 7. Klicken Sie auf die Schaltfläche **[Als Zielwerte übernehmen]**.
 - ⇒ Das Zertifikat wird in der Spalte „Zielwerte“ angezeigt.
 8. Markieren Sie das Kontrollfeld „Automatic Renewal“, wenn das Zertifikat automatisch erneuert werden soll. Eine automatische Erneuerung ist nur möglich, wenn der Controller mit einem Enrollment-Server verbunden ist.
 9. Klicken Sie auf die Schaltfläche **[Ins Gerät schreiben]**, um die Änderung zu übernehmen.
 - ⇒ Das Zertifikat wird im Bereich Gerätestatus/-aktionen mit dem aus dem Feld „DistinguishedName“ übernommenen Namen angezeigt.
- ➔ Das Zertifikat kann jetzt verwendet werden.

7.6.2 Extern erstellte und signierte Gerätezertifikate laden

Extern erstellte und signierte Gerätezertifikate (Zertifikatsdatei und die zugehörige private Schlüsseldatei) können direkt in den Controller geladen werden.

Um eine extern erstellte und signierte Zertifikatsdatei und die zugehörige private Schlüsseldatei in den Controller zu laden, gehen Sie folgendermaßen vor:

1. Öffnen Sie im WBM oder im WAGO Device-Manager die Seite „Device Certificates“.

2. Klicken Sie im Bereich „Einstellungen“ in der Gruppe „DeviceCertificate Liste“ auf die Schaltfläche **[+ DeviceCertificate]**.
 - ⇒ Es wird ein neuer Eintrag „DeviceCertificate <n>“ angelegt.
 3. Öffnen sie im Feld „Certificate“ das Dropdown-Menü bei der Anzeige „Nicht gesetzt“.
 4. Wählen Sie den Menüpunkt **[Auswählen]**.
 - ⇒ Ein Dateimanager-Fenster wird geöffnet.
 5. Navigieren Sie zu der Zertifikatsdatei und importieren Sie diese.
 6. Geben Sie im Feld „Comment“ einen Namen für das Zertifikat ein. Dieser Name wird bei der Auflistung der Zertifikate als Kommentar angezeigt.
 7. Öffnen sie im Feld „Private Key“ das Dropdown-Menü bei der Anzeige „Nicht gesetzt“.
 8. Wählen Sie den Menüpunkt **[Auswählen]**.
 - ⇒ Ein Dateimanager-Fenster wird geöffnet.
 9. Navigieren Sie zu der Schlüsseldatei und importieren Sie diese.
 10. Markieren Sie das Kontrollfeld „Automatic Renewal“, wenn das Zertifikat automatisch erneuert werden soll. Eine automatische Erneuerung ist nur möglich, wenn der Controller mit einem Enrollment-Server verbunden ist.
 11. Klicken Sie auf die Schaltfläche **[Ins Gerät schreiben]**, um die Änderung zu übernehmen.
 - ⇒ Das Zertifikat wird im Bereich Gerätestatus/-aktionen mit dem aus dem Feld „Comment“ übernommenen Namen angezeigt.
- ➔ Das Zertifikat kann jetzt verwendet werden.

8 Diagnose

8.1 Diagnose über Anzeigeelemente

Verschiedene Anzeigeelemente auf dem Gerät zeigen den Geräte- und Systemstatus an. Die Anzahl, Ausführung und Anordnung der Anzeigeelemente ist produktspezifisch. Eine genaue Beschreibung der Diagnose über Anzeigeelemente finden Sie daher im Abschnitt "Diagnose über Anzeigeelemente" im jeweiligen Produkthandbuch.

8.2 Diagnose über WBM

Über den WAGO Device Manager können Sie verschiedene Diagnosefunktionen nutzen, um den Status des Gerätes zu ermitteln.

- Testen Sie die Verdrahtung des Gerätes (siehe [🔗 I/O-Check \[> 52 \]](#), [🔗 Verdrahtungstest durchführen \[> 96 \]](#)).
- Sehen Sie sich den Status des Gerätes bezogen auf bestimmte Einstellungen an. Sie finden den Gerätestatus im unteren Bereich „Gerätestatus/-aktionen“ der verschiedenen Register in der Ansicht „Einstellungen“.
- Sehen Sie sich den LED-Status des Gerätes in der Ansicht „Einstellungen“ im Register „LEDs“ an.
- Den Status der Applikation zeigt die LED-Anzeige „PLC“ im linken Bereich „Gerät“ an (siehe [🔗 Gerät \[> 51 \]](#)).
- In der Ansicht „Geräte-Log“ werden protokollierte Log-Einträge des Gerätes angezeigt (siehe [🔗 Geräte-Log \[> 63 \]](#), [🔗 Geräte-Log einsehen \[> 97 \]](#)).
- Aktuelle (Fehler-)Meldungen und Informationen während der Konfiguration finden Sie im Meldungsfenster (siehe [🔗 Meldungsfenster \[> 64 \]](#)).

8.2.1 Verdrahtungstest durchführen

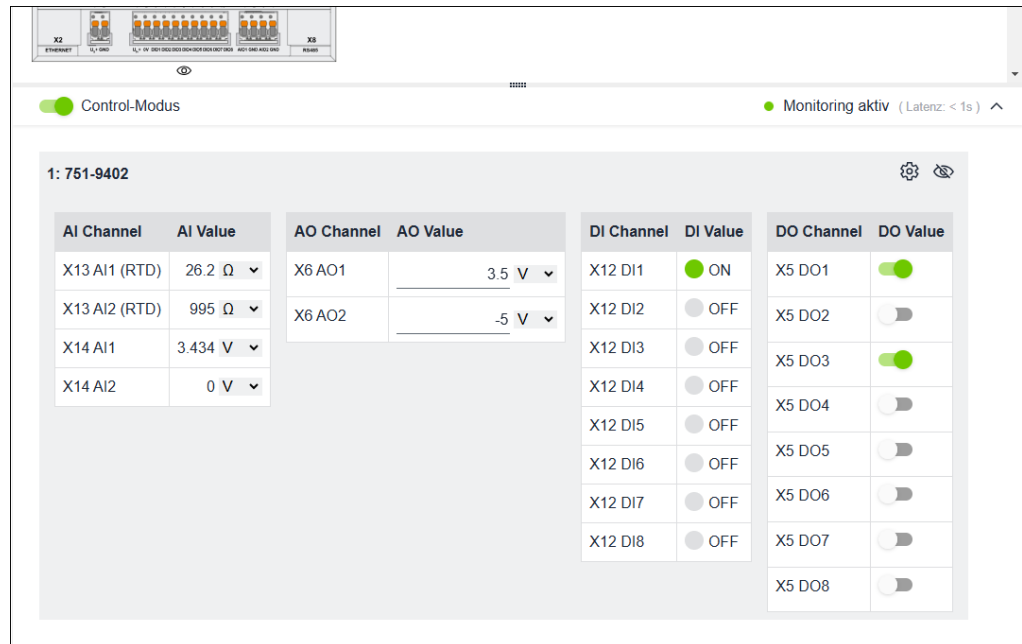
In der Ansicht I/O-Check können Sie einen Verdrahtungstest für konventionelle analoge und digitale Ein-/Ausgänge eines Gerätes durchführen. Es können testweise Ausgangssignale gesetzt werden („Control-Modus“) oder Eingangszustände in der entsprechenden physikalische Einheit eingelesen werden. Falls die Zustände am Gerät selbst visualisiert werden, z. B. über eine LED, dann wird der Zustand in Form einer farblich entsprechend hervorgehobenen LED dargestellt.

1. Öffnen Sie die Ansicht „I/O-Check“.
2. Klicken Sie auf das Augen-Icon  unter Ihrem Gerät.
 - ⇒ Das Monitoring wird aktiviert , d. h. die aktuellen Gerätewerte werden tabellarisch dargestellt.
 - ⇒ Die Latenz zeigt Ihnen den Aktualisierungszyklus der angezeigten Gerätewerte in Abhängigkeit von der Verbindung, Geräteauslastung oder anderen Faktoren an.
3. Vergleichen Sie die angezeigten Werte mit Ihrer Hardware, z. B. ob die grün dargestellte LED tatsächlich leuchtet.

4. Neben dem Monitoring können Sie ebenso Werte aktiv schreiben und lesen. Wechseln Sie dazu mit dem Schiebeschalter in den Control-Modus.



5. Verändern Sie einzelne Werte. Dazu verwenden Sie bei Analogausgangsmodulen Eingabefelder und bei Digitalausgangsmodulen Schiebeschalter.
- Hinweis:** Änderungen werden nicht gesammelt, das Schreiben erfolgt kontinuierlich während der Eingabe.



8.2.2 Geräte-Log einsehen

- Öffnen Sie das Register „Geräte-Log“.

Sie haben zwei Möglichkeiten, Log-Einträge einzusehen:

- Um Log-Einträge des Gerätes direkt im Register „Geräte-Log“ anzuzeigen, klicken Sie auf **[Log-Einträge abrufen]**.
- Um Log-Einträge des Gerätes abzurufen und in einer Datei zu speichern, wählen Sie zunächst das gewünschte **Datei-Ausgabeformat** („TXT“ oder „CSV“). Klicken Sie anschließend auf **[Log-Einträge als Datei abrufen]**.
 - ⇒ Standardmäßig werden die letzten 100 Log-Einträge angezeigt bzw. gespeichert, die mindestens den Log-Level „Informational“ besitzen.

Log-Einträge filtern

Sie haben verschiedene Möglichkeiten, Log-Einträge zu filtern und somit lange Listen zu reduzieren.

- Geben Sie eine **maximale Anzahl von Einträgen** vor:
bis zu 1.000 Log-Einträge bei direkter Anzeige oder bis zu 100.000.000 Log-Einträge bei Speicherung in einer Datei.

- Wählen Sie den **Log-Level** aus, der mindestens angezeigt werden soll.
Log-Level bezeichnen den Schweregrad bzw. die Dringlichkeitsstufe eines Log-Eintrages.
Tipp: Welche Log-Level generell protokolliert werden, konfigurieren Sie über das Register „Einstellungen“ > „Logging“.
- Geben Sie eine Zeichenkette ein, nach welcher die **Log-Quellen** der Einträge gefiltert werden sollen.
- Wählen Sie den **Zeitpunkt**, ab welchem Log-Einträge angezeigt werden. Setzen Sie dazu einen Haken in das Kontrollkästchen und wählen Sie Zeit und Datum über das Kalenderwidget aus.

Logging konfigurieren

Das Register „Geräte-Log“ dient zum Anzeigen und Filtern von Log-Einträgen. Welche Ereignisse generell vom Gerät geloggt werden, konfigurieren Sie in einem anderen Bereich der Oberfläche:

1. Öffnen Sie das Register „Einstellungen“.
2. Öffnen Sie die Seite „Logging“.
3. Ändern Sie hier beispielsweise, dass bereits ab einem Log-Level „Debug“ Log-Einträge erstellt werden.
4. Außerdem können Sie die für die Log-Einträge reservierte Speichergröße anpassen.
5. Auf der Seite „RemoteLogging“ können Sie bei Bedarf einen externen Logging-Server verbinden.

8.3 Systemintegrität prüfen

Das System kann auf Anforderung eine Prüfsumme über die Konfiguration berechnen.

Die Berechnung kann über die Schaltfläche **[Calculate Config Checksum]** auf der Seite „Information“ im WBM oder im WAGO Device Manager oder über die WDX-Methode „Security/CalculateConfigChecksum“ erfolgen.

Die Prüfsumme bleibt gleich, wenn die Konfiguration nicht geändert wird.

Das Ändern und Wiederzurückändern von Parametern kann zu einer unterschiedlichen Prüfsumme führen.

Vorgehensweise zur Prüfung:

1. Erzeugen sie die Prüfsumme der Konfiguration.
2. Lassen Sie sich die Prüfsumme anzeigen.
3. Notieren Sie Prüfsumme und bewahren Sie sie für spätere Vergleiche auf.
4. Wiederholen Sie den Vorgang regelmäßig, um durch Vergleichen der Prüfsummen unautorisierte Änderungen in der Konfiguration zu erkennen.
5. Erzeugen Sie nach jeder autorisierten Änderung die Prüfsumme und bewahren Sie sie auf (s. o.).

Tabellenverzeichnis

Tabelle 1	„Gerätestatus/-aktionen“ – „Security“	23
Tabelle 2	„Einstellungen“ – „Accountmanagement/PasswordQuality“	24
Tabelle 3	„Gerätestatus/-aktionen“ – „AccountManagement“	25
Tabelle 4	„Einstellungen“ – „SystemUser 2 (admin)“	25
Tabelle 5	„Gerätestatus/-aktionen“ – „AccountManagement“	26
Tabelle 6	„Einstellungen“ – „SystemUser 1 (root)“	26
Tabelle 7	„Einstellungen“ – „User Liste“	27
Tabelle 8	„Einstellungen“ – „UserRole Liste“	27
Tabelle 9	„Einstellungen“ – „OAuth2Server“	29
Tabelle 10	„Gerätestatus/-aktionen“ – „OAuth2Server“	30
Tabelle 11	„Einstellungen“ – „Logging“	31
Tabelle 12	„Einstellungen“ – „RsyslogClientConfig 1“	32
Tabelle 13	„Gerätestatus/-aktionen“ – „Identity“	32
Tabelle 14	„Gerätestatus/-aktionen“ – „Version“	33
Tabelle 15	„Einstellungen“ – „Timezone“	33
Tabelle 16	„Gerätestatus/-aktionen“ – „UTC“	33
Tabelle 17	„Gerätestatus/-aktionen“ – „Local Device Time“	33
Tabelle 18	„Einstellungen“ – „NTPClient“	34
Tabelle 19	„Einstellungen“ – „CertStore/CA“	37
Tabelle 20	„Einstellungen“ – „CACertificate Liste“	37
Tabelle 21	„Einstellungen“ – „CertificateRevocationList Liste“	37
Tabelle 22	„Gerätestatus/-aktionen“ – „CertificateRevocationList Liste“	37
Tabelle 23	„Einstellungen“ – „DeviceCertificate Liste“	38
Tabelle 24	„Einstellungen“ – „CertStore/EnrollmentServer“	38
Tabelle 25	„Gerätestatus/-aktionen“ – „CertStore/Device“	38
Tabelle 26	„Gerätestatus/-aktionen“ – „DeviceCertificate Liste“	39
Tabelle 27	„Gerätestatus/-aktionen“ – „IdentityCertificate <n>“	39
Tabelle 28	„Einstellungen“ – „Webserver“	39
Tabelle 29	„Einstellungen“ – „WebserverApplication <n>“	40
Tabelle 30	„Einstellungen“ – „WebserverCORSPolicy <n>“	40
Tabelle 31	„Gerätestatus/-aktionen“ – „FOSSModule Liste“	41
Tabelle 32	„Einstellungen“ – „WAGODeviceAccess“	41
Tabelle 33	„Gerätestatus/-aktionen“ – „FactorySettings“	42
Tabelle 34	Betriebsartenschalter	42
Tabelle 35	Reset-Taster	43
Tabelle 36	„Einstellungen“ – „USBServiceInterface“	44

Tabelle 37	Prozessabbild – Analogeingänge AI1, AI2	44
Tabelle 38	Prozessabbild – Prozesswerte AI; 0 ... 10 V; 16 Bit; WORD	44
Tabelle 39	Prozessabbild – Prozesswerte AI; –10 ... +10 V; 16 Bit; WORD	44
Tabelle 40	Prozessabbild – Prozesswerte AI; 0 ... 20 mA; 16 Bit; WORD	45
Tabelle 41	Prozessabbild – Prozesswerte AI; 4 ... 20 mA; 16 Bit; WORD	45
Tabelle 42	Prozessabbild – Prozesswerte AI; 3,6 ... 21 mA; 16 Bit; WORD	45
Tabelle 43	Prozessabbild – Analogein-/ausgänge AIO1, AIO2	45
Tabelle 44	Prozessabbild – Prozesswerte AO; 0 ... 10 V; 16 Bit; WORD	46
Tabelle 45	Prozessabbild – Prozesswerte AO; –10 ... +10 V; 16 Bit; WORD	46
Tabelle 46	Prozessabbild – Prozesswerte AO; –12 ... +12 V; 16 Bit; WORD	46
Tabelle 47	Prozessabbild – Prozesswerte AO; 0 ... 20 mA; 16 Bit; WORD	47
Tabelle 48	Prozessabbild – Prozesswerte AO; 0 ... 22 mA; 16 Bit; WORD	47
Tabelle 49	Prozessabbild – Prozesswerte AO; 4 ... 20 mA; 16 Bit; WORD	47
Tabelle 50	Prozessabbild – Temperatureingänge PT1+/PT1–, PT2+/PT2–	47
Tabelle 51	Prozessabbild – Prozesswerte RTD; Pt100, Pt200, Pt500, Pt1000; –200 ... +850 °C; 16 Bit; INT	48
Tabelle 52	Prozessabbild – Prozesswerte RTD; Ni100, Ni1000 (Tk6180), Ni1000 (TK5000); –60 ... +250 °C; 16 Bit; INT	48
Tabelle 53	Prozessabbild – Prozesswerte RTD; Ni120; –80 ... +260 °C; 16 Bit; INT	48
Tabelle 54	Prozessabbild – Prozesswerte RTD; Potentiometer; 0 ... 1200 Ohm; 16 Bit; INT	49
Tabelle 55	Prozessabbild – Prozesswerte RTD; Potentiometer; 0 ... 5000 Ohm; 16 Bit; INT	49
Tabelle 56	Prozessabbild – Digitaleingänge DI1 ... DI8	49
Tabelle 57	Prozessabbild – Prozesswerte digitale Eingänge – BOOL	49
Tabelle 58	Prozessabbild – Digitalein-/ausgänge DIO1 ... DIO8	49
Tabelle 59	Prozessabbild – Prozesswerte digitale Eingänge – BOOL	50
Tabelle 60	Prozessabbild – Prozesswerte digitale Ausgänge – BOOL	50
Tabelle 61	Icons und Bedienelementen der Ansicht „Einstellungen“	60
Tabelle 62	Datei-Handling	60
Tabelle 63	„Einstellungen“ – „Bridge Configuration“	67
Tabelle 64	„Einstellungen“ – „Bridge 1 ... Bridge <n>“	67
Tabelle 65	„Einstellungen“ – „Networking/StormProtection“	68
Tabelle 66	„Einstellungen“ – „EthernetPort 1 ... EthernetPort <n>“	68
Tabelle 67	„Gerätestatus/-aktionen“ – „Bridge <n> (br<n-1>)“	69
Tabelle 68	„Gerätestatus/-aktionen“ – „EthernetPort <n> (X<n>)“	69
Tabelle 69	„Einstellungen“ – „FirewallMACFilterRule Liste“	71
Tabelle 70	„Einstellungen“ – „FirewallIPFilterIncomingRule Liste“	71
Tabelle 71	„Einstellungen“ – „FirewallIPFilterForwardingRule Liste“	72
Tabelle 72	„Einstellungen“ – „IKEConnection“	74

Tabelle 73	„Einstellungen“ – „IPsecTunnel“	74
Tabelle 74	„Gerätestatus/-aktionen“ – „IPsecTunnel“	74
Tabelle 75	„Einstellungen“ – „Automount“	76
Tabelle 76	Voreinstellung ETHERNET-Kommunikation	79
Tabelle 77	„Einstellungen“ – „Accountmanagement/PasswordQuality“	80

Abbildungsverzeichnis

Abbildung 1	Zwiebelschalenmodell (Beispiel)	14
Abbildung 2	Referenzarchitektur	15
Abbildung 3	Grafische Benutzeroberfläche	51
Abbildung 4	Verbundenes Gerät.....	52
Abbildung 5	Ansicht „I/O-Check“ (Beispiel)	53
Abbildung 6	Statusanzeige des Gerätes (Beispiel).....	53
Abbildung 7	Statusanzeige der Kanäle (Beispiel)	54
Abbildung 8	Monitormodus aktiv (Beispiel)	55
Abbildung 9	Control-Modus aktiv (Beispiel).....	56
Abbildung 10	Ansicht „Einstellungen“ (Beispiel)	57
Abbildung 11	Ansicht „Neustart“	61
Abbildung 12	Ansicht „Firmware“	61
Abbildung 13	Ansicht „Backup/Restore“	62
Abbildung 14	Register „Geräte-Log“	64
Abbildung 15	Meldungsleiste	65
Abbildung 16	Meldungsfenster	65
Abbildung 17	Register „Geräte-Log“	78

WAGO GmbH & Co. KG

Postfach 2880 · D - 32385 Minden
Hansastraße 27 · D - 32423 Minden

✉ info@wago.com
🌐 www.wago.com

Zentrale
Vertrieb

Auftragsservice

+49 (0) 571/887 – 0
+49 (0) 571/887 – 44 222
+49 (0) 571/887 – 44 333

WAGO ist eine eingetragene Marke der WAGO Verwaltungsgesellschaft mbH.

Copyright – WAGO GmbH & Co. KG – Alle Rechte vorbehalten. Inhalt und Struktur der WAGO Websites, Kataloge, Videos und andere WAGO Medien unterliegen dem Urheberrecht. Die Verbreitung oder Veränderung des Inhalts dieser Seiten und Videos ist nicht gestattet. Des Weiteren darf der Inhalt weder zu kommerziellen Zwecken kopiert, noch Dritten zugänglich gemacht werden. Dem Urheberrecht unterliegen auch die Bilder und Videos, die der WAGO GmbH & Co. KG von Dritten zur Verfügung gestellt wurden.